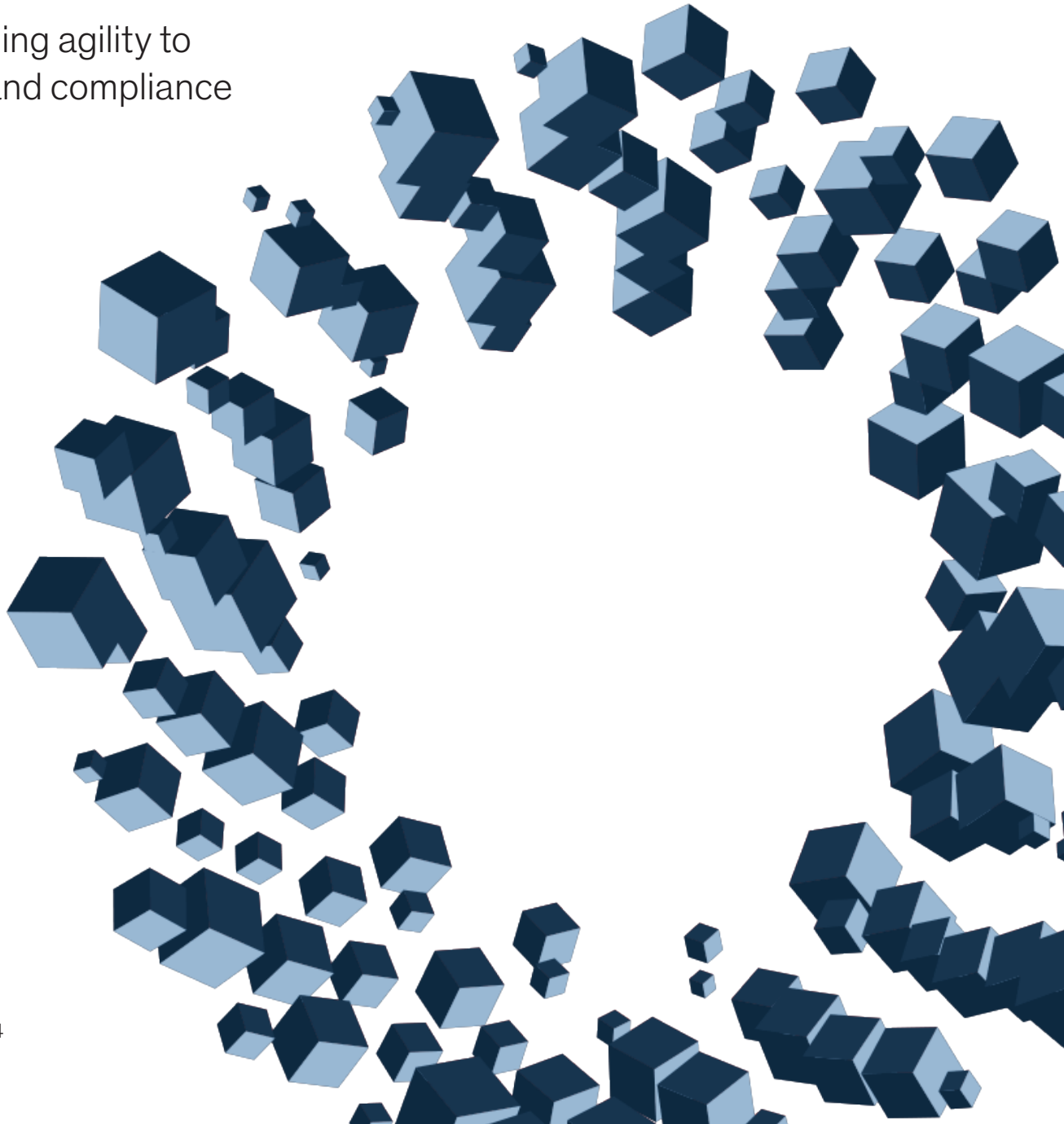
McKinsey & Company

McKinsey on Risk & Resilience

Strengthening agility to guide risk and compliance



Number 17, July 2024

The articles in *McKinsey on Risk & Resilience* are written by risk experts and practitioners from McKinsey's Risk & Resilience Practice and other firm practices. This publication offers readers insights into value-creating strategies and the translation of those strategies into company performance.

This issue, and future issues, are available to registered users online at McKinsey.com. Comments and requests for copies or for permissions to republish an article can be sent via email to McKinsey_Risk@McKinsey.com.

Cover image:
© olaser/Getty Images

Contents

Introduction

As we enter the second half of the year, risk leaders continue to face a set of challenges not seen in decades—and some never seen before.

Sadly, peace and security has resurfaced as a top priority for chief risk officers and their colleagues. Global conflict is at its highest level since the end of the Cold War, and combined with a geopolitical landscape that will see elections in 60 countries and across 50 percent of the world's population by year end, the existing and potential shifts in the world order cannot be ignored.

This geopolitical fragmentation, along with a continuous fight against inflationary pressures and related interest rate volatility (which increases the cost of debt), comes with rising cybersecurity threats; new technology risks, such as those from generative AI; climate change; and more. Together, these challenges have complicated—and, in some cases, made obsolete—strategies planned just a few months ago and show the need for a strategic level of risk and resilience across industries.

In this issue of McKinsey on Risk & Resilience, we not only examine the tests risk and compliance face today and in the future but also provide actionable tactics for mitigating these hazards and navigating them in a way that can spur growth and competitive advantage.

We address the shifting geopolitical space by introducing the concept of structural segmentation, a cluster of moves that global corporations are considering to help mitigate geopolitical exposure, enable locally informed decision making, and clear a pathway to safe, stable growth.

On the issue of interest rates, we offer a playbook for banks and other institutions to help them meet today's uncertainty and answer a critical question: can risk managers retain the benefit of higher rates while preparing for cuts and managing the potential for macroeconomic surprises?

Similarly for insurers, our team offers strategies for mitigating interest rate volatility and other risks, with a special emphasis on climate risk—another modern threat that already has had a significant impact on the industry.
In our work with the Institute of International Finance, we identify emerging technologies' potential to enhance and transform institutions and how to manage these technologies safely, decreasing the potential for bad actors to take advantage of new systems.

Our team in Europe examines new European Union regulations aimed at curtailing digital risk for financial institutions. While this suite of new regulations comes as no surprise, most financial institutions must address a gap in compliance. We suggest ways institutions can bridge those gaps effectively and cost-efficiently.

Last, in our ongoing and comprehensive examination of generative AI, we explore how this technology can have an outsize impact on improving outcomes in credit customer assistance—a function that has emerged as a top focus of regulators and institutions post pandemic.

Together, these analyses underscore the extreme and, in many ways, unprecedented variability besieging the risk office and its institutions. The good news is that agile organizations, guided by risk and compliance, can thrive in this environment by remaining resilient.

We hope you enjoy these articles and find in them ideas worthy of application. Let us know what you think at McKinsey_Risk@McKinsey.com and on the McKinsey Insights app.

Thomas Poppensieker
Senior partner and chair,
Global Risk & Resilience Editorial Board

Can your company remain global and if so, how?

Geopolitical uncertainty is forcing global companies to take a hard look at the decades-long strategy of geographic expansion.

by Andrew Grant, Michael Birshan, Olivia White, and Ziad Haider

Rising geopolitical tensions are testing the resilience of global organizations and challenging existing growth strategies. Wars in Europe and the Middle East and escalating US–China competition have the attention of the executive suite and the boardroom. Global business leaders are asking, "What is the future of the global corporation? Do we need to fundamentally shift strategies and structure?"

These questions are being asked amid a measurable decline in global cooperation on peace and security and slowing cooperation in other areas, as reflected in a new global cooperation barometer released by the World Economic Forum and McKinsey in January (Exhibit 1). The intensity and duration of conflicts worldwide are at their highest levels since before the end of the Cold War[1]: 183 active conflicts in 2023, with violent events last year increasing by 28 percent and fatalities by 14 percent.[2]

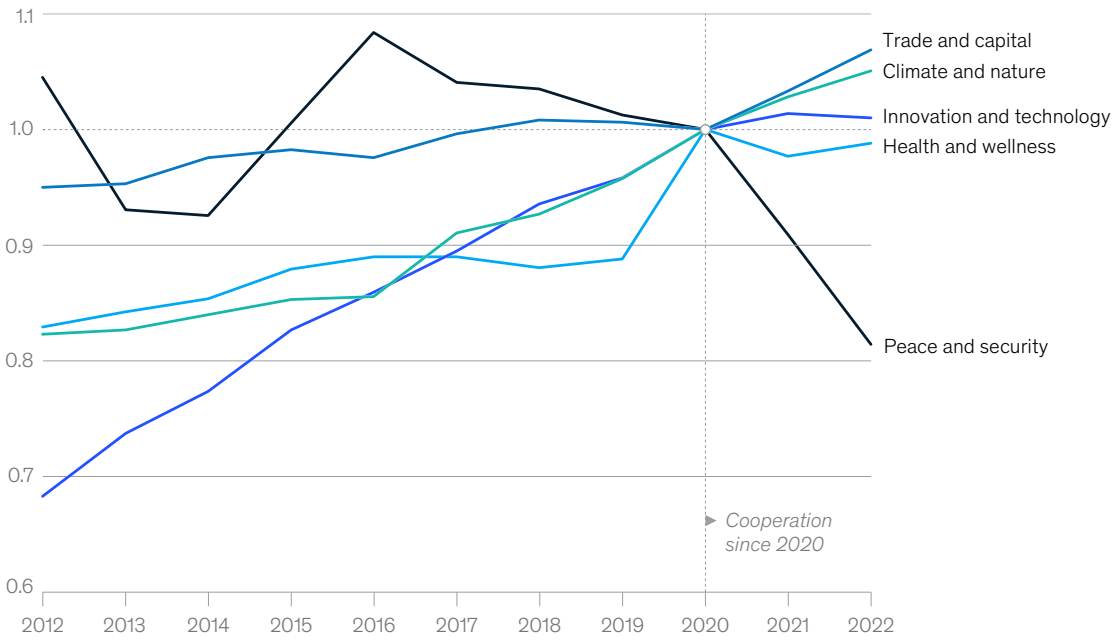
Moreover, 2024 is the year of national elections, with more than 60 countries and nearly 50 percent of the global population heading to the polls.[3] Even if only a subset of these elections lead to shifts in leadership and policy, business leaders cannot ignore political uncertainty against the backdrop of an evolving global order.

[1] Emma Beals and Peter Salisbury, "A world at war: What is behind the global explosion of violent conflict?," *Foreign Affairs*, October 30, 2023.
[2] *The Armed Conflict Survey 2023*, first edition, Abingdon, United Kingdom: Routledge, 2023.
[3] Koh Ewe, "The ultimate election year: All the elections around the world in 2024," *Time*, December 28, 2023.

Exhibit 1

Peace and security among nations have eroded sharply since 2020.

Average index of cooperation metrics, 2020 = 1



McKinsey & Company

Unsurprisingly, business leaders view geopolitics as the top risk to global growth and view political transitions as the leading emergent risk, according to our latest global economic survey (Exhibit 2). Business leaders tell us diverging regulatory requirements, increased in-market risk in multiple geographies, and the need to establish local bona fide units without generating undue risk to the parent are the reasons that now, as one executive we spoke to put it, "Geopolitics trumps capital markets."

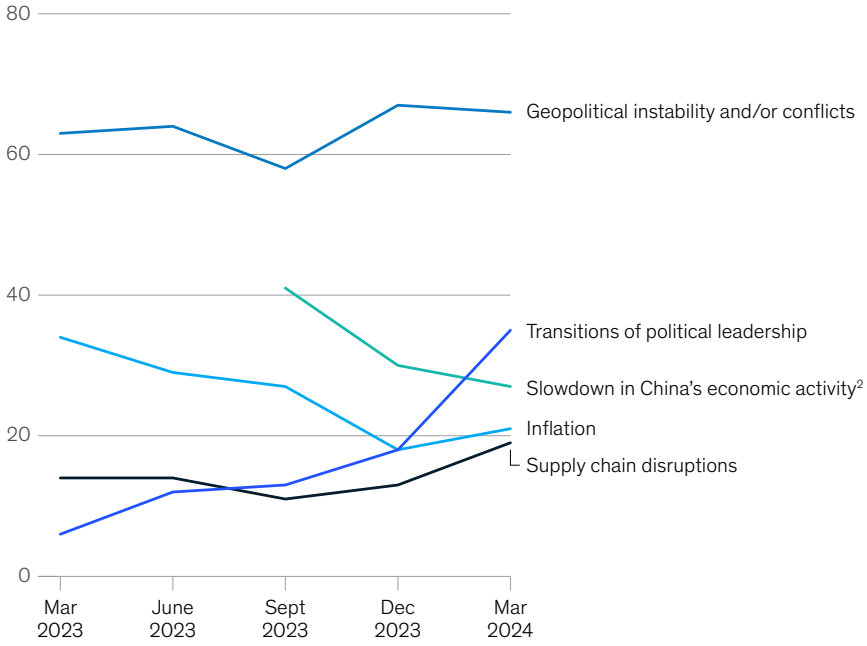
Given this environment, one of the biggest strategic questions confronting global business leaders today is, "How global can my organization remain?" The cost of getting this question wrong is high; assets, growth, value creation, and, most importantly, people may be at risk. At the same time, there is a real advantage to getting it right. In a changing geopolitical landscape, organizations can differentiate themselves through the strategic courage with which they navigate this era of volatility.

Our analysis shows that business leaders can take a systematic approach to building what we call geopolitical resilience. One element of that approach is conducting geopolitical-scenario planning, thinking through a set of "black swans, gray rhinos, and silver linings"—unpredictable and probable high-impact events, as well as potential opportunities amid the storm clouds. A second element involves upgrading board capabilities on geopolitical risk.

Exhibit 2

Geopolitical instability tops the list of concerns for global business leaders.

Biggest potential risks to global economic growth, next 12 months,[1]
% of respondents



[1]Out of 15 potential risks that were presented as answer choices. Respondents were able to select up to 3 answer choices. Mar 27–31, 2023, n = 871; June 5–9, 2023, n = 1,044; Aug 31–Sept 8, 2023, n = 997; Nov 27–Dec 1, 2023, n = 942; Mar 4–8, 2024, n = 957.
[2]Not included in the list of potential risks in the Mar 2023 and June 2023 surveys.
Source: McKinsey Global Surveys on economic conditions, 2023–24

McKinsey & Company

There is another emerging aspect of geopolitical resilience that increasingly arises in our conversations with business leaders—one that we refer to as "structural segmentation." Structural segmentation describes a cluster of moves that global corporations are considering to mitigate geopolitical exposure, to enable locally informed decision making, and to clear a pathway to safe, stable growth.

In what follows, we define structural segmentation, identify questions for global companies to consider as they calibrate their operating models, and outline specific examples of how firms are implementing a segmentation approach. The findings are based on our and our colleagues' conversations with business leaders across the world, as well as on analysis of more than 100 global organizations' strategic moves.

Structural segmentation for geopolitical resilience

During the past 25 years, geographic boundaries have faded for companies. Many built complex supply chains that shipped components and products across the world, often crisscrossing it multiple times. Wisely, they established global R&D hubs, forged enterprise-wide technology stacks, democratized access to data, consolidated legal entities, and fostered one-firm cultures.

The premise of a fully globalized world, which underpinned these moves, is now in question, and companies should respond. Legal, regulatory, economic, political, and social contexts are shifting. Companies are increasingly seeking an integrated approach to taking coordinated action across six domains: operations (that includes production and supply chains), R&D, technology and data, legal entity structure, capital, and people. Across each of these domains, we find that organizations typically contemplate either (re)committing to globality or structurally segmenting activities across geopolitically distant markets.

Structural segmentation can take several forms across a continuum. Full structural segmentation involves localizing parallel activities in multiple locations across the world. Factories, for example, may produce only for the regions in which they are located (often in a region or regions that have higher "geopolitical distance"[4] from the company's home market).

As an alternative, some companies are relocating toward home or geopolitically aligned countries, at least in select domains. In general, this involves preserving global connections—for example, housing most technologies in a home country, while creating a minimal viable footprint in geopolitically distant countries. In its most extreme form, however, this might include a major move, such as housing all R&D in the home market.

The intent is to respond to geopolitical realities while preserving the benefits of global reach and seizing opportunities for resilient growth. Just as scenario planning is not a crystal ball, so structural segmentation is not a magic wand. It is, however, a strategic and operational choice that companies may contemplate to survive and thrive in a new era. Although there is a range of ways multinationals can employ segmentation, there are six main areas:

Reshaping production and supply chains for resilience

Escalating geopolitical competition and disruptions induced by COVID-19, weather, and conflict have made supply chains a top priority issue for C-suites and boardrooms. Organizations are deploying or exploring a variety of segmentation strategies, considering both geopolitical exposures and concentrated production or supply chain footprints.

Some companies have responded by recommitting to a global approach. This typically does not mean ignoring a changing world order but rather moving toward greater strategic diversification, whereby a company moves away from a concentrated global supply chain to a model that sources from and

[4] Geopolitical distance between countries can be measured by examining the countries' observable behavior on foreign policy issues, such as through their voting behavior in the United Nations General Assembly.

produces in a greater range of markets across the world. The idea is that a broader and arguably more global web of connections adds resilience, since it is not dependent on any one region or country.

Multinational companies that instead opt for structural segmentation in operations seek to make sure that production and supply could survive if one region were to be cut off. So far, companies have attempted to localize across multiple regions to various degrees. Some have declared an "in market, for market" strategy, building localized production and supply chains so that in-market supply meets in-market demand as much as possible. Others have opted for a market-plus strategy, which entails a substantial footprint and supply chain—for both domestic and export purposes—in one region, supplemented by imports and exports as needed from other geographies.

Few companies are considering complete localization or the relocation of their entire production from one geography to another. Those that do so tend to only have a few affected product lines and focus on only the most sensitive portions of their supply chains. Indeed, as all goods supply chains start where resources come out of the ground, there is a natural limit to how much of a supply chain a company can practically relocate.

Many firms are considering some degree of structural segmentation, however. A recent European Central Bank survey of multinationals with significant operations in the European Union, for instance, reports that 42 percent of firms plan to "friend-shore" production over the next five years, in contrast to only 11 percent that reported having done so in the past five years.[5] Similar trends emerge in supply chains. Our 2023 survey of supply chain leaders found two-thirds of respondents sourcing more from suppliers located closer to their production sites last year.[6]

While reshaping footprints and supply chains can segment geopolitical risk, it comes with costs and complexity. Some organizations may struggle to replicate supplier networks in new markets because of factors such as labor shortages and infrastructure limitations. For others, diversification efforts may only shift concentration risk from one tier of suppliers to another, without significantly reducing overall risk. A third challenge is the stickiness of supply chains. Even as many multinationals, for example, are expanding their footprints in geographies such as Southeast Asia, China's export share to ASEAN economies is also continuing to grow. That results in the deepening use of components made in China by multinationals in some supply chains.[7]

Ring-fencing research and development

With technology top of mind for business and world leaders, multinationals are having to adapt their R&D footprints. They can no longer rely on open access to talent and should balance geopolitical, regulatory, reputational, and commercial factors. Organizations may wrestle with questions such as where they should conduct R&D, who is conducting it, and with whom they should share it.

On one end of the spectrum of structural segmentation, some companies are seeking to fully localize their R&D in multiple regions. A leading life sciences company, for example, has opted to build parallel R&D efforts in two different markets that are geopolitically distant from each other. That way, it can sustain access to top talent in each market and preserve—and possibly enhance—its flexibility to develop products that meet varying local requirements.

---

[5] Maria Grazia Attinasi et al., "Global production and supply chain risks: Insights from a survey of leading companies," *ECB Economic Bulletin,* 2023, Volume 7.

[6] Knut Alicke, Tacy Foster, Katharina Hauck, and Vera Trautwein, "Tech and regionalization bolster supply chains, but complacency looms," McKinsey, November 3, 2023.

[7] *Geopolitics and the geometry of global trade,* McKinsey Global Institute, January 17, 2024.

Other companies are moving assets toward their home markets. Leading US technology companies are home- and friend-shoring researchers in sensitive technology domains, fully moving them away from markets that are geopolitically distant from the United States.

In the middle of the spectrum, some companies are maintaining R&D operations in markets that are geopolitically distant from the location of their headquarters. But they are introducing strict guardrails, including restrictions in technology arenas that are part of the strategic competition between nations or have multiple use applications like quantum computing and applied AI.

Companies that use these strategies often find they can not only mitigate risk but also gain a competitive advantage. A local R&D presence can make products more tailored to market-specific consumer preferences, fueling a global organization's local growth strategy. While the approaches vary, the motivating factor is the same: to build geopolitical resilience while preserving an edge in innovation.

Derisking technology stacks and data lakes

A unified global technology stack was once seen as a source of competitive advantage as companies sought to win through scale at low cost. Now, this strategy is under stress from multiple sources: the proliferation of data protection, privacy, and localization laws around the world; the increasing threat of data theft, malevolent-technology insertion, and espionage; and concerns about the overconcentration of data in markets where threats are present.

As a result, companies are revisiting their enterprise technology stacks and considering rebalancing their traditional approach to technology and data management. Some businesses are opting to adopt a globally optimized footprint, subject to local regulations, even if this involves hosting technology services in high-risk markets and accepting the associated additional geopolitical risk. A leading consumer company, for instance, took a local regulatory change as an impetus to localize its e-commerce stack, thereby improving in-market customer experience while managing compliance with the new regulation.

Increasingly, other companies are structurally segmenting their enterprise technology stacks in various forms. Collectively, the moves seek to adapt technology and data location to geopolitical and regulatory demands. Many are shifting toward structural segmentation not just to accommodate individual geographies but also to take a holistic approach to managing broader geopolitical risks, including those related to intellectual property theft and data appropriation.

One approach is to invest in a fully localized IT domain and separate sensitive data from high-risk markets. Our research shows many US companies, from private equity to professional services, are actively exploring or executing on efforts to fully decouple their tech stacks in sensitive regions. These moves follow escalating geopolitical competition and new expectations from customers and public stakeholders.

Even firms that have stopped short of full localization are introducing architecture changes, storing data in states that are geopolitically close to the location of their headquarters—subject to local regulations. Companies taking this approach aim to create a minimal viable technology footprint in geopolitically distant countries that then complies with the data and privacy laws of those countries. Cloud providers, for example, are developing new platform governance processes while disconnecting some markets from their global infrastructure backbones. Software companies in advanced fields like AI, the Internet of Things, and edge computing are separating these sensitive capabilities from their global offerings, often in partnership with local providers, to manage information security.

Creating decision-making distance through legal entities

Organizations are rethinking the role of legal entities and the part they play in navigating geopolitical challenges. Business leaders who have revisited their entity structures cite diverging regulatory requirements, increased in-market risk, and the intent to be seen as a local player.

One example of legal segmentation is an international defense company that redesigned its entities to enable it to operate as a local contractor in each of its major markets. Leadership and decision making are handled locally, while equity remains with the global parent.

Creating distance from the parent, however, can come with its own set of new challenges: functions are duplicated, costs rise, risk appetite between the parent and local units diverges, global culture can erode, and efficiencies are traded off.

In addition to these ramifications, there is a risk that entity segmentation may not be enough to offset geopolitical risk. The parent and segmented entity may still be viewed as one and the same—albeit now with potentially inadequate governance and risk controls.

Some companies have therefore gone further, judging that a continued overall parent was untenable. A leading law firm, for instance, has established a stand-alone unit for its in-country operations. Leading venture capital firms also have split off their regional businesses into new entities with distinct brands and local boards. In these cases, of course, the benefits of operating globally will be lost, and in some cases, a fully separated business unit has also turned into a major competitor in some markets.

Sometimes the same company has had to make more than one of these moves across the globe in a market-differentiated manner. One of the world's largest food and beverage companies, for example, is seeking to reacquire global ownership over one of its local franchises in the Middle East. It entered into a minority stake in a joint venture partnership with a local operator in China and later increased its stake, noting the need to anchor its partnership structure and to continue capturing increased demand in an important market. Lastly, the company fully exited and sold off its operations in Russia following Russia's invasion of Ukraine, citing the humanitarian crisis caused by the war and the unpredictable operating environment that rendered continued operations untenable and inconsistent with its values. From global ownership to local strategic partnerships to wholesale exit, this company has had to contend with multifactorial geopolitics and customize and evolve its approach across essential markets—a level of agility that global companies may need to develop.

Safeguarding capital invested in geopolitically distant regions

Geopolitical shifts affect capital flows. The International Monetary Fund, for example, reports that increases in geopolitical distance between two nations are associated with reduced investment.[8] Since 2015, direct investment in China and Russia has dropped precipitously, as a result of decreased spending from advanced economies in Asia, Europe, and the United States.[9] However, flows into other developing economies have increased, notably into Africa, India, and developing Europe (Exhibit 3).

In this environment, many global companies are selecting some form of structural segmentation, strengthening the geopolitical lens through which they examine capital decisions—be it the capital intensity of their business models or the capital structures by which they are financed.

Some companies are using a localization strategy, adjusting financing so cash inflows and outflows are exposed to similar geopolitical conditions: for example, financing the purchase of aircraft leased to airlines in a country with debt from banks in that same country.

An alternative approach is to move toward home, shifting capital away from more geopolitically distant regions. To retain connections in these markets, some firms have shifted toward partnerships and ecosystem plays and away from direct, tangible capital investment. The aim is to mitigate the risk of stranded or written-off assets, while bringing a local market's talent, networks, and capital to a venture. Other companies are taking capital off the table in higher-risk markets

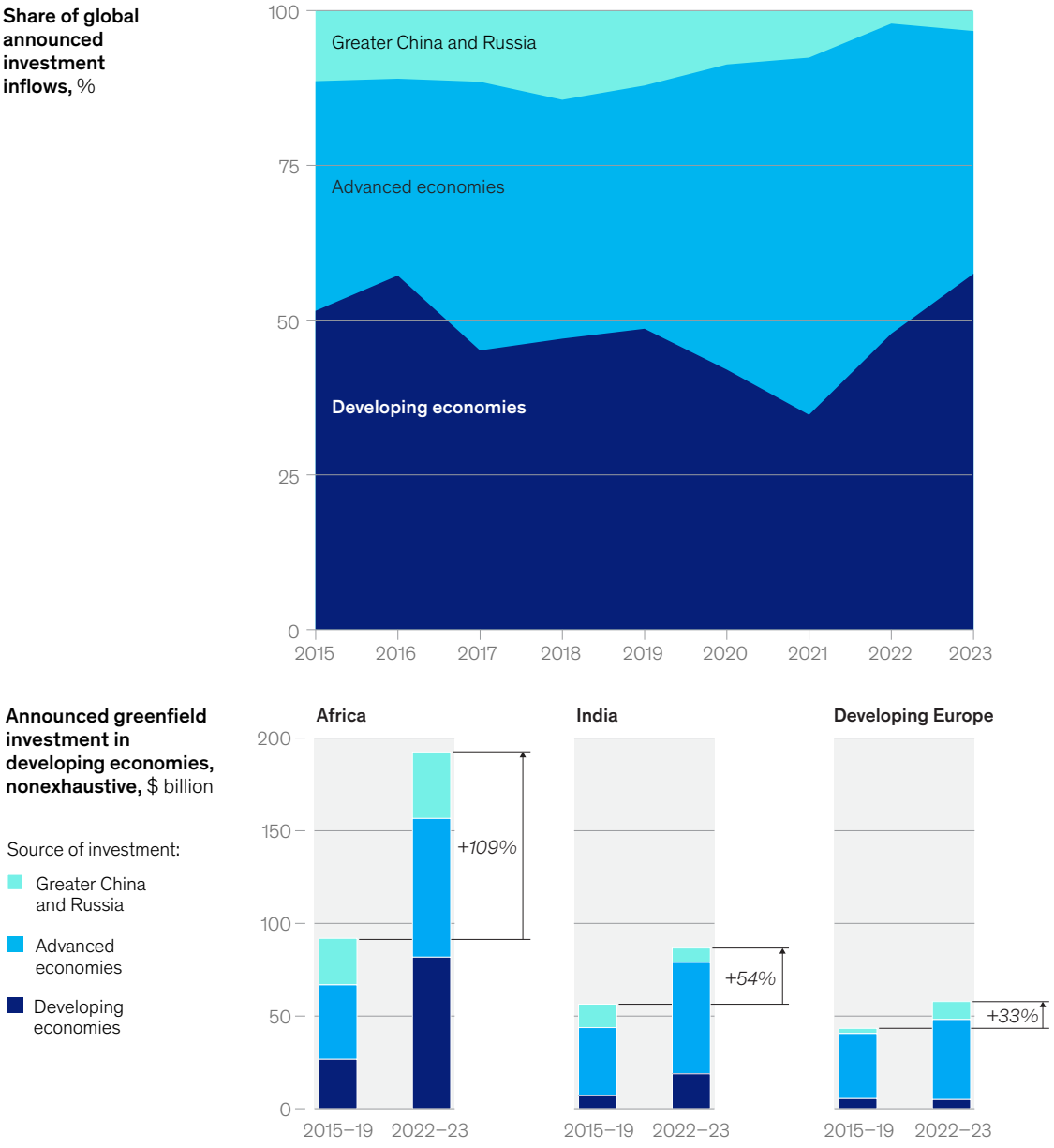
[8] *Global financial stability report: Safeguarding financial stability amid high inflation and geopolitical risks,* International Monetary Fund, April 2023.
[9] *Geopolitics and the geometry of global trade,* McKinsey Global Institute, January 17, 2024.

through liquidity events—such as IPOs, private sales, and share sell-downs—including to other international investors that are less geopolitically distant from the market in question. A number of global consumer goods companies, for example, have sold or leased fixed in-country assets, such as manufacturing plants and warehouses, to trusted local partners; these exchanges are underpinned by long-term contracts to enable supply chain stability.

Exhibit 3

Global investment is shifting.

Capital flows have moved to Africa, India, and developing Europe



Note: Data for 2022–23 is through Oct 2023.
Source: fDi Markets (a service from the Financial Times 2023; all rights reserved); McKinsey Global Institute analysis

McKinsey & Company

Securing people and connections

The extent to which an organization can remain global is a question that is most delicate when it concerns people and culture. In keeping a workforce secure, organizations should find balance. They should preserve long-standing and cherished principles of global connectivity and a one-firm culture. But at the same time, they should address the crucial need to maintain robust screening and insider risk programs and reassure geopolitically concerned stakeholders of adequate people-related processes.

The reality is many multinationals do not have a choice in instituting some measure of structural segmentation with people; stakeholders ranging from government officials to customers increasingly expect them to do so. Some approaches include shifting the staff's home office locations, changing travel policies and protocols so that staffing pools are more localized by region, segmenting access to data on global networks from certain markets, and creating firewalls for certain communications outside market.

Organizations that conclude they need to implement such approaches should do so with care to avoid singling out a set of colleagues and, thereby, eroding the global fabric of the organization. Previous McKinsey research has shown that organizations that can operate as "one firm" are 2.3 times more likely to be in the top quartile of health and high-performing organizations.[10] Accordingly, multinationals may, for example, choose to limit discussions on geopolitically sensitive topics to senior leaders in headquarters, as well as to the top in-country leadership, to avoid inflaming internal sentiment and risking leaks that could trigger a market backlash.

Additionally, given the internal scrutiny that such segmentation approaches can generate, many multinationals are having to think equally hard about how to continue fostering a sense of global connectivity not only for cultural reasons but also for talent retention. One leading US firm that we spoke with has sought to shore up cultural cohesion by purposefully bringing the entirety of its incoming class of employees from a geopolitically distant market to global headquarters for shared learning and connectivity.

Business leaders know that healthy organizations that are inclusive and deeply connected can better deal with external change and crises. The challenge today, however, is fostering that sense of inclusivity and connection when geopolitical risk mitigation can demand segmenting the organization's global operating model in ways that create purposeful distance.

Emerging playbooks for structural segmentation

Broadly, we find that businesses typically adopt one of two postures—recommitting to a single global strategy or moving toward structural segmentation—and use it to guide decision making across each of the six dimensions. That said, companies do have the flexibility to follow a singular approach across all areas or otherwise adopt a more mixed set of tactics.

While every company's circumstances—and, hence, optimal response—are different, some archetypes are emerging. Asset-light companies require limited assets in-market to generate large revenues. These businesses might decide to follow a global approach to operations and capital, as their risks are inherently lower, while potentially segmenting technology stacks and legal entity structures to support agility in a volatile geopolitical context. More capital-intensive companies are progressively introducing (or at least thinking hard about how to introduce) greater segmentation across multiple dimensions, notably operations and supply chains, often with a market-plus strategy. Financial franchises present a special case: delegating decision making to semiautonomous regional entities and sourcing capital locally allows segmentation that both reduces geopolitical risk and accelerates growth.

[10] Blair Epstein, Caitlin Hewes, and Scott Keller, "Capturing the value of 'one firm,'" *McKinsey Quarterly,* May 9, 2023.

Businesses with long-standing presences in geopolitically distant markets have more complex choices. Their de facto postures emerged out of decisions made during the last three decades. Given the costs incurred to establish their presences, these firms are more likely to stick with their current postures or change more incrementally—with segmentation occurring around the edges, dimension by dimension. The result is a mixed strategy: for example, implementing a segmented tech stack but doubling down on a global approach to people, R&D, and capital.

In setting their postures, business leaders should consider both risk management and growth strategy, as well as execution feasibility, of course. While they are more commonly reported on, not all structural-segmentation decisions have been made to reduce risk; quite a number have been made to, at least in part, enable more locally tailored and therefore resilient growth strategies in geopolitically distant markets.

Finally, these dimensions of structural segmentation play out at the market level, but deciding where a market starts and stops requires thought. Is the segmentation meant for a single country, a few countries—and if so, can they be treated together, or does each require distinct postures against the segmentation dimensions—or a broad swath of the world?

For leaders dealing with today's volatile geopolitical environment, Peter Drucker's maxim is more apt than ever: "The greatest danger in times of turbulence is not the turbulence; it is to act with yesterday's logic."

Structural segmentation is today's logic, one that business leaders are exploring both to navigate geopolitical headwinds and to potentially secure growth. Indeed, navigating the new geopolitics and geometry of global trade requires business leaders to conduct multifactorial calculus and at times develop market-differentiated approaches to structural segmentation. What structural segmentation is not, however, is a magic formula to eliminate all risk. Geopolitically distant regions by their nature present risk, as well as opportunity. Multinational companies must be prepared for greater scrutiny of their operating models globally, no matter how thoughtful a segmentation approach they may employ.

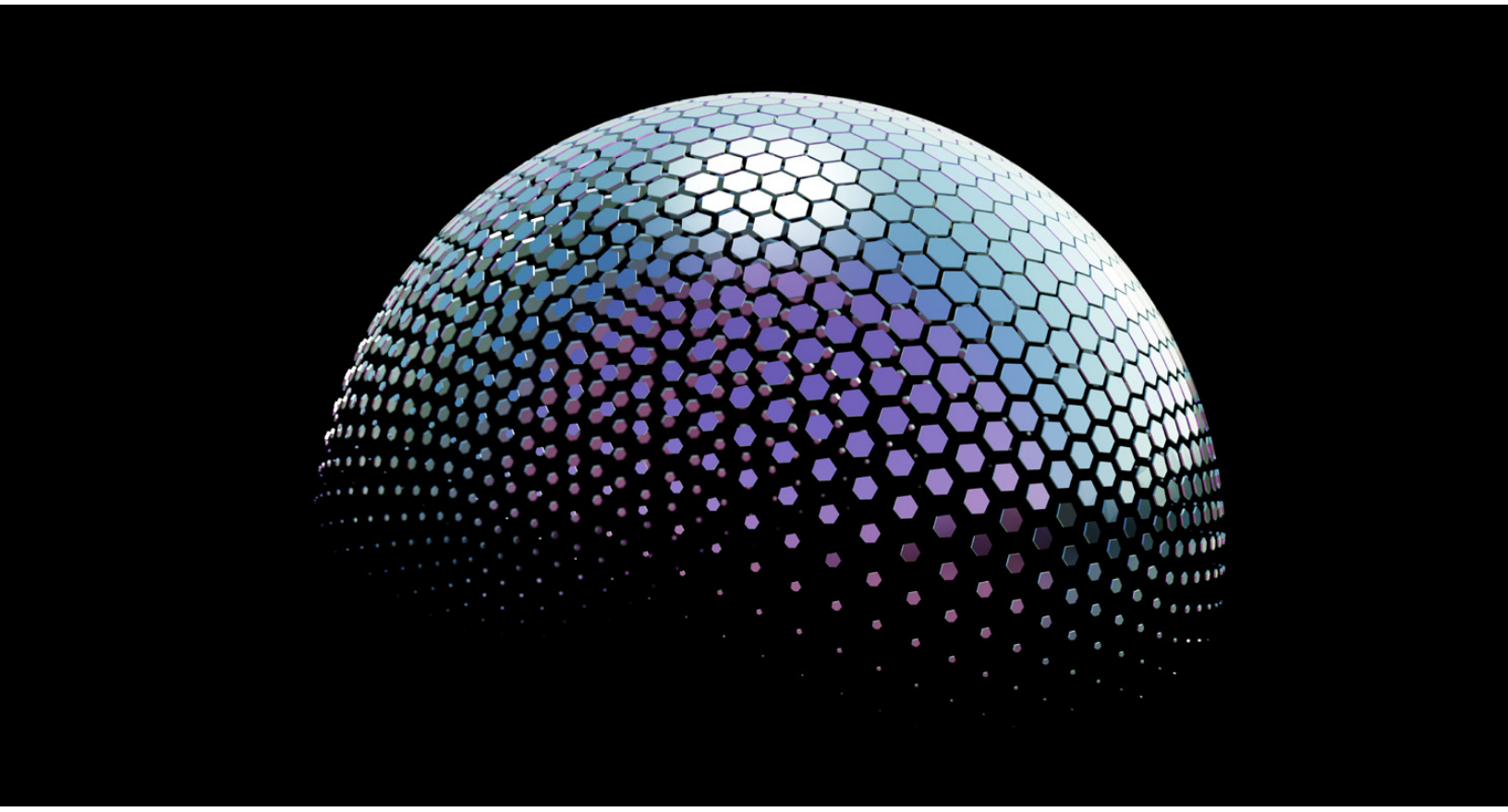
Andrew Grant is a senior partner in McKinsey's Auckland office, **Michael Birshan** is a senior partner in the London office, **Olivia White** is a director of the McKinsey Global Institute and a senior partner in the Bay Area office, and **Ziad Haider** is the global director of geopolitical risk and a partner in the Singapore office.

The authors wish to thank Knut Alicke, Tucker Bailey, Raphael Bick, Mike Doheny, Ben Fletcher, Henry Frear, Axel Karlsson, Lucas Lim, Karol Mansfeld, Jean-Christophe Mieszala, Brooke Weddle, Lola Woetzel, and Carter Wood for their contributions to this article.

Europe's new resilience regime: The race to get ready for DORA

As the directive for the European Union's Digital Operational Resilience Act approaches, financial institutions and their providers of information and communications technology have significant work ahead, a new McKinsey survey shows.

This article is a collaborative effort by Jim Boehm and Sebastian Schneider, with Florian Stoll, Lucy Shenton, and Nils Motsch, representing views from McKinsey's Risk & Resilience Practice and McKinsey Digital.



Digitalization of the financial sector has brought significant benefits but has also exposed businesses to rising technology risks, including cyberattacks, system outages, and third-party information and communications technology (ICT) failures. To ensure financial institutions (FIs) remain resilient in the face of these threats, the European Union's Digital Operational Resilience Act (DORA) sets out detailed requirements for EU-based FIs to protect their key business processes (see sidebar "DORA's scope"). While DORA has some overlap with other regulations (such as BAIT and VAIT in Germany[1]), it is the first regulation of its kind to focus on digital resilience across the European financial ecosystem.

As DORA's enforcement date of January 17, 2025, approaches (some regulatory requirements are not yet finalized), McKinsey has conducted a survey with major European financial institutions and critical ICT third parties to understand their progress in achieving DORA compliance. The results are mixed: most institutions have started the journey, but many will need to do more to meet their obligations on time. In this article, we explore some of the most pressing issues highlighted in our survey, and we reflect on the steps that have put some institutions on a more promising DORA compliance path than that of their peers.

DORA implementation: Where does the industry stand?

European FIs and critical ICT service providers still have time to align their resilience capabilities with DORA requirements—but the window is closing. Our survey finds that 94 percent of FIs are fully engaged in understanding the detailed requirements of the legislation; most are doing so through a dedicated DORA program, with DORA as a board-level agenda item (see sidebar "How one large European financial company tackled the DORA challenge").

[1] Bankaufsichtliche Anforderungen an die IT (BAIT) and Versicherungsaufsichtliche Anforderungen an die IT (VAIT) are the banking supervisory requirements and the insurance supervisory requirements for IT in Germany.

DORA's scope

The DORA regulation comprises five main content chapters, supported by two batches of regulatory technical standards (RTSs) and implementing technical standards. In total, the documents contain more than 600 pages and 1,100 lines of requirements relevant to financial institutions and ICT third parties. The chapters of the final text focus on the following components:

- *ICT risk management* requires an internal risk-management framework and strategy; risk tolerance; policies, procedures, and protocols; and an independent control function.
- *ICT-related incident management, classification, and reporting* involves defining, establishing, and implementing a process to manage and record incidents and cyberthreats—and to centralize reporting.
- *Digital operational resilience testing* mandates a risk-based approach to all testing, including physical testing, application testing, technology resilience ("switchover") testing, and threat-led penetration testing (TLPT).
- *Management of third-party risk* requires an ICT risk-management framework, third-party register, risk assessments, analysis of concentration risk, and continued monitoring and auditing of ICT third-party service providers that support critical business services.
- *Information-sharing arrangements* allow FIs to exchange cyberthreat information and intelligence and require them to notify competent authorities of information-sharing arrangements.

How one large European financial company tackled the DORA challenge

An EU-based, market-leading financial institution with operations in more than 50 countries had just completed a major technology risk-remediation program in 2023 and had to rapidly shift efforts to meet DORA requirements. In the fourth quarter of 2023, the organization established a small DORA program focused on compliance in a few defined areas, but it lacked the ability to scale and execute across the group in a risk-based way, given the highly complex intrafunctional and geographic setup. In addition, some senior stakeholders had a lack of focus, and working-level teams were misaligned.

Not wanting to lose momentum from its highly successful 2023 remediation efforts and knowing how much ground it had to cover to meet the DORA expectations, the company redoubled its DORA program efforts, starting at the very beginning of the first quarter of 2024, and set a target to meet the regulation's requirements by January 2025. It completely redesigned its program by defining specific activity clusters focused on each of the regulation's content areas, reorganizing governance and steering to include business and technology leaders across all key entities, and establishing enterprise-wide tracking and reporting of progress and documentation in a centralized tooling solution. Notably, it also brought all of its operating entities under the same program orchestration umbrella for end-to-end support and execution management. The company was highly efficient in those activities: it achieved its redesigned program structure within one month (more than 300 staff members onboarded, full planning and gap assessment complete). Now with a better, more holistic structure in place, it turned to the activation plan.

Key to its successful activation was the strong sense of accountability the company placed on its delivery leaders: the activity cluster leads, plus the single points of contact for each operating entity. That approach had dual effects: the company drove strong execution of DORA-related activities, of course; more significantly, it created a culture of technology risk management throughout the organization, while training and upskilling the entire staff.

By taking such strong, positive steps—both toward central, strategic orchestration and planning *and* toward action-oriented, leader-driven accountability for delivery—the company has started to see tech risk management not as a "nonfunctional task" but, instead, as a key driver of business value. This truly strategic, business- and risk-based, holistic, structured approach has set the company on a much steeper DORA preparation trajectory than that of its peers across Europe.

As of April 2024, most organizations say they have completed a gap analysis and are in the process of designing or rolling out implementation programs. Nevertheless, every organization reports some uncertainty—for example, around the precise requirements of the legislation. In particular, respondents point to two challenges:

— limited clarity on the scope of key items (for example, the definitions of critical or important functions [CIFs] and of critical ICT third-party providers)

— concern over the timeline for implementation, considering that the second of two batches of the European Supervisory Authorities' regulatory technical standards (RTSs) is only set to be finalized in July 2024, and that some regulatory requirements (for example, updating all relevant third-party contracts) require significant lead time for implementation

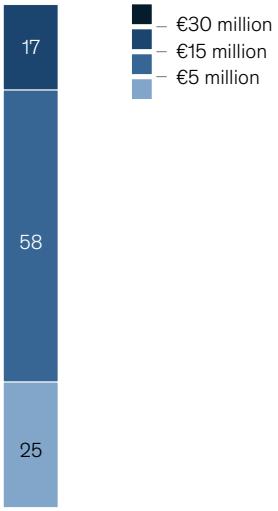
Regarding the first challenge, one chief information security officer said, "The breadth of the DORA program, given the broad range of topics, is unavoidable. However, the chosen depth of scoping significantly impacts the size of effort required to achieve compliance."

At some institutions, uncertainty over scoping has led to increased budget allocations (Exhibit 1). Typically, an institution might have earmarked €5 million to €15 million for its DORA program strategy, planning, design, and orchestration. But early estimates for full implementation costs are coming in at five to ten times that range. One large FI reported that its final planned DORA implementation spend across the group amounted to nearly €100 million, split between program orchestration and technology control upgrades. According to our conversations with other FIs, we expect similar multiples across the financial industry—particularly at large companies or those that struggle to adopt a risk-based approach to scoping.

Exhibit 1

Most surveyed institutions plan to spend €5 million–15 million on Digital Operational Resilience Act strategies, planning, design, and orchestration.

Planned spending to comply with Digital Operational Resilience Act requirements,[1]
% of respondents (n = 12)



[1]1-off costs to reach compliance.
Source: McKinsey survey on Digital Operational Resilience Act (DORA) program readiness, 18 executives and DORA program leaders from leading EU financial institutions and information and communications technology service providers, Mar 2024

McKinsey & Company

When it comes to DORA program capacity, about 40 percent of financial entities and ICT providers dedicate more than seven full-time equivalents (FTEs), while less than 20 percent have yet to assign dedicated FTEs (Exhibit 2). In our client engagements, several leading organizations say the broad scope of DORA requirements means that different functional areas are driving deliverables, albeit with central coordination. All told, these factors tend to reduce the number of dedicated FTEs.

Program steering is a vital cog in the implementation machine, but our research gives little indication that the industry has arrived at a standardized approach. At about 50 percent of surveyed institutions, the IT organization drives DORA implementation, whereas among the remaining group, a mix of business and oversight functions more commonly take control (Exhibit 3). The prevalent ownership distribution suggests many organizations still see digital resilience as an "IT problem" rather than a groupwide concern.

Regulatory compliance is rarely inexpensive, and most survey respondents feel that maintaining DORA compliance will incur ongoing costs. Among our survey respondents, 70 percent say continuing to meet DORA requirements will result in permanently higher run costs for technology and technology control.

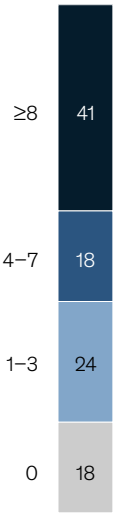
Challenges facing industry participants and ICT service providers

Of the many challenges facing institutions, one that stands out in our survey responses is ICT third-party risk management (Exhibit 4). To manage third-party risk effectively, financial institutions must make significant efforts on two fronts: ensuring comprehensive oversight of all ICT service providers and their associated risk and proactively managing the digital risk associated with critical ICT third-party service providers. To achieve these goals in a cost-effective, end-to-end manner, leading FIs take a risk-based and holistic approach, in turn requiring dedicated processes and technologies.

Exhibit 2

Companies dedicate varying numbers of full-time employees to their Digital Operational Resilience Act–compliance programs.

Number of full-time employees dedicated to Digital Operational Resilience Act program,
% of respondents (n = 17)



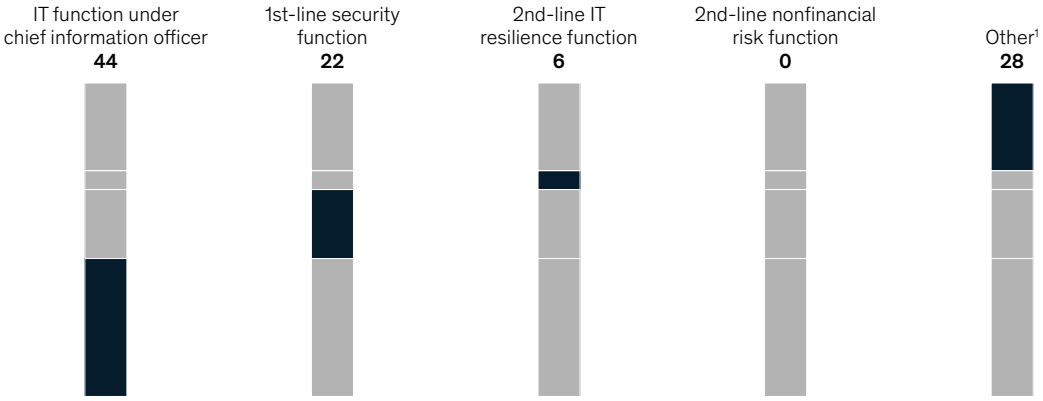
Note: Figures do not sum to 100%, because of rounding.
Source: McKinsey survey on Digital Operational Resilience Act (DORA) program readiness, 18 executives and DORA program leaders from leading EU financial institutions and information and communications technology service providers, Mar 2024

McKinsey & Company

Exhibit 3

Organizational responsibility for driving alignment with the Digital Operational Resilience Act is often in the IT function.

Organizational function responsible for alignment with Digital Operational Resilience Act,
% of respondents (n = 18)



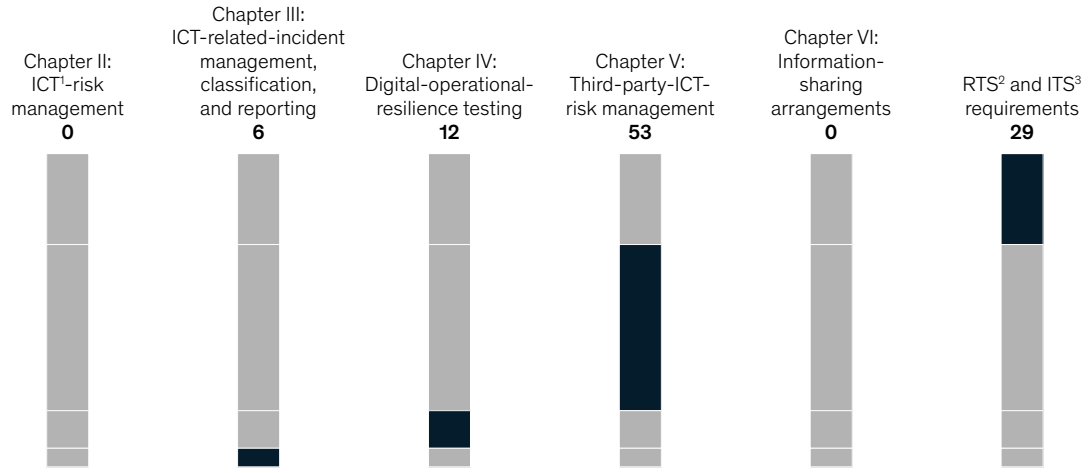
[1]Includes 1st-line function under COO, 2nd-line nonfinancial risk function, and combination of multiple functions, among others.
Source: McKinsey survey on Digital Operational Resilience Act (DORA) program readiness, 18 executives and DORA program leaders from leading EU financial institutions and information and communications technology service providers, Mar 2024

McKinsey & Company

Exhibit 4

Management of third-party information and communications technology risk is seen as a key challenge.

Most complex element of Digital Operational Resilience Act to fulfill, % of respondents (n = 17)



[1]Information and communication technology.
[2]Regulatory technical standards.
[3]IT services.
Source: McKinsey survey on Digital Operational Resilience Act (DORA) program readiness, 18 executives and DORA program leaders from leading EU financial institutions and information and communications technology service providers, Mar 2024

McKinsey & Company

Once more, a key variable is scoping, and our discussions with major FIs show wide variation in understanding of the legislation's scope—even among companies working with similar numbers of ICT vendors. For example, in contract remediation, some organizations are focusing on as few as 20 remediations, whereas others plan to remediate as many as 3,000 contracts (see sidebar "Key scoping items for DORA remediation activities").

An important factor in making remediation decisions is how to define a "critical" ICT third-party service provider. Under Article 31 of DORA, criteria for consideration include systemic impact on stability, continuity and quality of provision of financial services, the number of institutions relying on the provider, and interdependencies among institutions. Organizations must work closely with legal counsel to determine which interpretation of that definition optimally fulfills DORA requirements and boosts digital resilience.

In terms of engagement with third parties, many FIs report challenges when negotiating with smaller entities. One difficulty is that smaller third parties often lack sufficient talent or resources to achieve full DORA compliance and, thus, may struggle to meet requirements on time. Such variations in capabilities among organizations are likely to lengthen the time frame for some implementation programs.

A common structural challenge for a financial institution is in its dual role of engaging with providers and being a provider for others. For instance, a financial institution may offer payments services on behalf of another financial institution, while also using third parties to support its own business services. These twin dynamics can expose the institution to regulatory scrutiny from two angles: it may need to both initiate and respond to contract remediation exercises.

Key scoping items for DORA remediation activities

Below are key scoping areas companies should consider when assessing their DORA compliance.

— *Defining critical or important functions (CIFs).* Accurately defining CIFs is a cornerstone of DORA scoping (for example, mapping of IT assets to CIFs, defining recovery times). The challenge for institutions is that no industry-wide framework determines which functions should be deemed as CIFs. Instead, industry participants tend to rely on individual third-party frameworks, such as BaFin's RRP (recovery and resilience plan) or the Bank of England's IBS (important business services), and on the European Banking Authority's technical guidance.

— *Scoping ICT service providers.* DORA defines an ICT service provider as "an undertaking providing ICT services; digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services, which include the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services." Given this broad language, it is up to market participants themselves to decide whether individual ICT providers meet the definition. Some decision makers believe that services provided by companies outside traditional IT, such as law firms and consultancies, could fall within the legislation's scope; some, however, do not. In addition, organizations often lack a consolidated view of third-party relationships across business units, geographies, parents/subsidiaries, or group/legal entities. Such lack of alignment could yield different classifications of the same provider, causing confusion during an onsite examination.

— *Understanding feasible and acceptable recovery times for different scenarios.* Financial entities report challenges in determining appropriate target recovery time objectives (RTOs) and recovery point objectives. For example, achieving four-hour recovery times (a standard RTO) would be reasonable in the event of a small, contained incident, but it would be nearly impossible after a large-scale ransomware attack leading to a major outage. Leading organizations take a use case and criticality-oriented approach to set recovery times, often tied to business impact analyses.

— *Defining and choosing appropriate test scenarios to conduct threat-led penetration testing.* Some organizations say they struggle to define the right test scenarios for TLPT, a particular concern when testing critical or important functions. It may make sense to agree on a joint definition of critical scenarios, or on a respective sharing/recognition of testing results with critical third-party providers—or on both.

Across the industry, timing is likely to be a significant concern in the months ahead. In our survey, just about a third of financial institutions express confidence that they can fulfill all DORA regulatory expectations by January 2025. Moreover, all expect at least some DORA efforts to continue beyond then (Exhibit 5). Even those that believe they can achieve compliance by January 2025 say that implementation and rollout into "business as usual" across geographies will continue beyond the legal enforcement date.

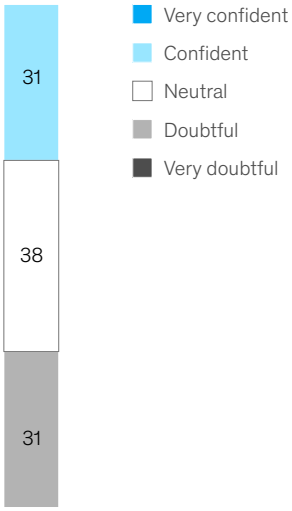
Taking action: Four strategic imperatives

Preparations for DORA will continue to accelerate in the coming months. As decision makers navigate the process, best practice will be not only to focus on complying with the regulation, but also to reflect broader business goals. We have seen some leading organizations anchor their efforts on four strategic principles.

Exhibit 5

Surveyed institutions are uncertain that they can meet the Digital Operational Resilience Act deadline.

Organizational confidence in fulfilling all Digital Operational Resilience Act regulatory expectations by Jan 2025,
% of respondents (n = 16)



Source: McKinsey survey on Digital Operational Resilience Act (DORA) program readiness, 18 executives and DORA program leaders from leading EU financial institutions and information and communications technology service providers, Mar 2024

McKinsey & Company

See the regulation as a resilience opportunity rather than a tick-box exercise

As many as 80 percent of remediation programs fail because they lack a strategic foundation. To prevent DORA programs from succumbing to the same fate, decision makers need to see the program for what it can be: a transformational opportunity to reorganize and enhance processes, tools, and technologies, while boosting resilience. But if institutions simply update policy documents and define system mappings to do the bare minimum, they risk turning their DORA programs into paper tigers—inflating costs with limited impact beyond paper. If, conversely, institutions implement DORA with digital resilience as an objective—by using their DORA program to identify and eradicate ICT risk at scale—they will create a fundamentally stronger financial ecosystem and improve customer trust.

Make resilience business-led

As in many transformative projects, leadership is a critical enabler. We see two vital building blocks:

— *Drive the transformation from the top.* For an effective transformation, senior managers need to formulate a clear strategy, enhanced by programmatic support structured around the business and its priorities. Regulators' expectations will be relevant in this context. In one recent examination, the regulator requested evidence that IT risk-management efforts were business-led and involved leaders from the business. Our experience suggests that linking regulatory remediation deliverables to business objectives is key to measuring resilience success, which is possible only when business colleagues are at the helm in driving implementation.

— *Appoint a single accountable program owner.* While DORA affects multiple functions, a single accountable owner provides a point of coordination and steering. This approach will sharpen strategic oversight and lead to better prioritization and communication throughout the program.

Scope astutely: Take a risk-based approach; define 'done' clearly

From our survey, scoping is a significant challenge—and opportunity—as DORA preparations reach their final stages. Our surveyed FIs commonly report struggling with seemingly unending regulatory programs that "boil the ocean" in terms of interpreting and meeting regulatory expectations, consequently with ever-growing scope and costs.

Organizations that precisely define the regulation's risk-based aims are most likely to execute effectively. They engage in two best practices:

— *Implementing requirements based on risk.* Leading companies take a risk-based approach to resilience, identifying their most critical processes and prioritizing capability requirements according to risk. This means not creating "one control requirement set to rule them all" but defining risk-differentiated policies and controls based on the business value of different processes. Such an approach yields a more streamlined, efficient application of DORA requirements, optimizing both DORA spend and time to compliance.

— *Explicitly defining "done": when DORA requirements are met and risk is mitigated*. Often in the course of regulatory and remediation programs, organizations run into the challenge of proliferating requirements and ever-lengthening timelines. That may occur when internal stakeholders seek to add their own priorities to the list, increasing the effort required. By agreeing from the outset on how to define "done," a company can save months of program extension, spend, and iteration.

Collectively collaborate to ensure systemic resilience

Business leaders may feel it is counterintuitive to collaborate with competitors on regulatory alignment, but information sharing can actually streamline the implementation process and build trusted networks. We have seen, time and again, the power and impact of cross-industry collaboration on security and regulatory topics. Consider these approaches:

— *Invest in information sharing and exchange; candidly communicate how you view scope requirements and challenges.* Given that DORA expressly aims to strengthen the resilience of the entire financial ecosystem, it should catalyze collaboration across the European financial industry. Lean into the fact that it makes sense for FIs to work together.

— *Use DORA to build digital trust.* ICT service providers and FIs can use DORA to boost transparency and build trust in their digital products and services. As quality, resilience, and security improve, so will uptime, access, and fraud-mitigation outcomes. Digital trust can become a value differentiator for customers.

As the deadline for DORA implementation approaches, financial institutions and ICT service providers have their work cut out to achieve the expected level of digital resilience. Scoping exercises and closure of gaps against the final text and RTS batches will demand significant attention in the months ahead.

That said, DORA also presents a valuable opportunity. Institutions have a chance to revisit critical challenges around digital resilience, bring diverse parts of the organization together, and transform fundamental capabilities that will maintain the resilience of the financial ecosystem. Given the systemic reach of digital technologies, financial institutions and ICT providers can work together to increase trust in the industry and create value for the long term.

Jim Boehm is a partner in McKinsey's London office; **Sebastian Schneide**r is a senior partner in the Munich office, where **Nils Motsch** is an associate partner; **Florian Stoll** is a consultant in the Frankfurt office; and **Lucy Shenton** is an associate partner in the Berlin office.

Banking on interest rates: A playbook for the new era of volatility

Five levers can help banks set themselves on a course to more proactive and effective interest rate risk management.

by Andreas Bohn and Sebastian Schneider, with Enrique Briega and Mario Nargi

The recent accelerated rise in global interest rates, the fastest in decades, brought the curtain down on an extended period of cheap money but provided little clarity on the longer-term outlook. In 2024, competing forces of tepid growth, geopolitical tension, and regional conflict are creating nearly equal chances of higher-for-longer benchmark rates and rapid cuts. In the banking industry, this uncertainty presents both risks and opportunities. But in the absence of recent precedent, many institutions lack the necessary playbook to tackle the challenge.

As rates have risen from their record lows, banks have in general profited from rising net interest margins (NIMs). However, if policy makers switch swiftly into cutting mode, banks may see the opposite effect. For now, futures markets predict the start of that process toward the end of 2024. In that context, the question facing risk managers is how they can retain the benefit of higher rates while preparing for cuts and managing the potential for macroeconomic surprises.

The volatility playing out in rates markets is reflected in bank deposit trends, with customers more actively managing their cash to make the most of shifting monetary conditions. In Europe, deposits reached 63 percent of available stable funding (ASF) in 2023, compared with 57 percent in 2021.[1] In the US, conversely, the share of deposits over total liabilities fell over a similar period as money migrated to investments such as money market funds.

In the face of accelerating deposit flows, McKinsey research shows that bank risk management and funding performance has been highly variable. Between 2021 and 2023, the best-performing US and EU banks saw interest rate expenses rise 70 percent less than at the worst-performing banks (Exhibit 1). Among the drivers were better deposit and interest rate management.

Alongside the impacts of deposit flows, funding has come under pressure from other factors, including the steady withdrawal of pandemic-related central

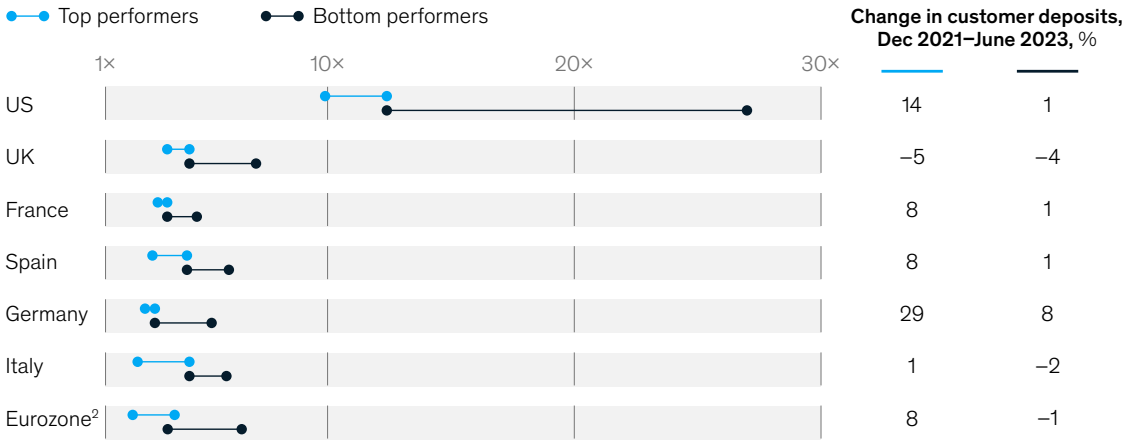
[1] *Monitoring of liquidity coverage ratio and net stable funding ratio implementation in the EU – third report*, European Banking Authority, June 15, 2023.

The question facing risk managers is how they can retain the benefit of higher rates while preparing for cuts and managing the potential for macroeconomic surprises.

Exhibit 1

Best-performing banks incur lower-interest-rate expenses and attract more deposits.

Increase in interest expenses by performance, Dec 2021–June 2023,[1] multiple



[1]Top performers defined as 10th–49th percentile of interest expense increases; bottom performers defined as 50th–90th percentile of interest expense increases. Percentiles 0–10 and 90–100 were outliers on the distribution and therefore excluded. US, n = 5; UK, n = 7; France, n = 8; Spain, n = 9; Germany, n = 16; Italy, n = 6; eurozone, n = 70.
[2]Eurozone includes banks from France, Spain, Germany, and Italy alongside banks from other eurozone countries.
Source: S&P Capital IQ; SNL Financial; McKinsey analysis

McKinsey & Company

bank liquidity facilities. Meanwhile, innovations such as instant payments have motivated customers to make faster and larger transfers. These withdrawals can happen quickly and be fueled by social media, creating a powerful new species of risk.

In the context of a more uncertain environment, regulatory authorities are doubling down on oversight of the potential impacts of rate volatility—for example, by asking banks to mitigate the potential effects of rate normalization, increasing overall scrutiny, and demanding evidence of methodology upgrades. Among European supervisory priorities for 2024–26, banks are advised to sharpen their governance and strategic frameworks to strengthen asset and liability management (ALM) and develop new funding plans and contingency measures for short-term liquidity shocks, including evaluating the adequacy of assumptions supporting some behavioral models.[2] In the same vein, the Basel Committee on Banking Supervision in 2023 proposed a recalibration of shocks for interest rate risk in the banking book. Banks can achieve this by extending the time series used in model calibration from the current December 2015 standard to December 2022, bringing more volatile rate distributions into the equation.

In a recent McKinsey roundtable, 40 percent of Europe, Middle East, and Africa bank treasurers said the topic that will attract most regulatory attention in the coming period is liquidity risk, followed by capital risk and interest rate risk in the banking book (IRRBB). With these risks in mind,

[2] "SSM Supervisory Priorities, 2024-2026," in *Supervisory priorities and assessment of risks and vulnerabilities*, European Central Bank, 2023.

34 percent of treasurers said their top priorities with respect to rate risk were enhancing models and analytics, revising pricing strategies on loans and deposits, and beefing up ALM governance and monitoring capabilities.

Most participants also expected treasury teams to get more involved in strategic planning and board engagement and to engage business units more closely to define pricing strategies and product innovation (Exhibit 2).

In response to these dynamics, we expect to see many banks revisiting the role of the treasury function in the months ahead. For many, this will mean moving away from approaches designed for the low-rate era and toward those predicated on uncertainty. In this article, we discuss how forward-looking banks are redesigning their treasury functions to obtain deeper insights into probabilities around interest rates and their impacts on pricing, customer behavior, deposits, and liquidity.

Five steps to enhancing the treasury function

To manage volatile interest rates more effectively, leading banks are revisiting practices in the treasury function that evolved during the low-interest-rate period and may no longer be fit for purpose—or at least should be updated for the new environment. Pioneers have taken steps in five broad focus areas: steering and monitoring, risk measurement and capabilities, stress testing, bank funding, and hedging.

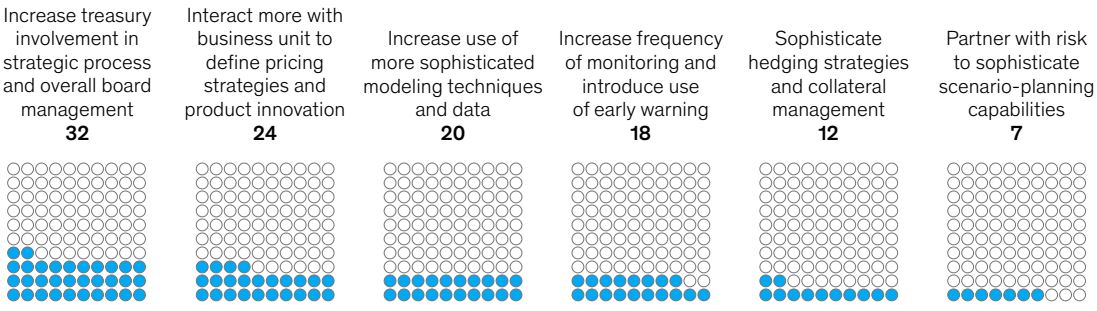
Build efficiency and sophistication

A precondition of effective oversight of interest rate business is to ensure decision makers have a clear view of the current state of play. Currently, the standard approach across the industry is somewhat passive, meaning it is based on static or seldom-reviewed pricing and risk management decisions, often taken by relationship managers. Models are fed with low-frequency data, and

Exhibit 2

Most banks expect more treasury involvement in strategic processes and more interaction with business units.

Expected change in treasury activities and capabilities over the next years, % of respondents listing option as top 3[1]



[1]Data gathered Nov 23, 2023; n = 29.

McKinsey & Company

banks use static fund transfer pricing (FTP) to calculate net interest margins. Monitoring often reflects regulatory timelines rather than the desire to optimize decision making.

Forward-looking banks are tackling these challenges through a more hands-on approach to steering and monitoring, including the following measures:

- dynamic reviews of FTP, reflecting microsegment behaviors and pricing strategies tied to customer lifetime value and the opportunity cost of liquidity
- increased product innovation to boost funding from both corporate and retail clients
- ensuring access to high-quality, frequent, and granular data, with systems equipped to send early warning signals on potential changes in customer behaviors, especially to capture early signs of liquidity shifts
- use of risk limits and targets as active steering mechanisms, bolstered by links to incentives
- automation of reporting and monitoring, so liquidity and other events can be scaled internally much faster, backed by real-time data where possible

Upgrade IRRBB measurement and capabilities

Leading banks are getting a grip on IRRBB risk in areas such as balance sheet management, pricing, and collateral. Many have assembled dedicated teams to help them make more effective decisions. Given the threat to deposits, some are making greater use of scenario-based frameworks, bringing together liquidity and interest rate risk management. They are using real-time data to inform funding and pricing decisions.

To ensure they consider all aspects of rate risk, leading banks employ a cascade of models, feeding the outputs into steering and stress-testing frameworks, and capturing behavioral indicators that can inform balance sheet planning and hedging activities. Some banks are employing behavioral models to forecast loan acceptance rates and credit line drawings. Best practice involves using statistical grids differentiated by type of customer, product, and process phase.

When it comes to loans, some banks are leveraging AI to predict prepayments and their impacts on balance sheets and hedging requirements. Best practice in prepayments modeling is to move away from linear models and toward machine learning algorithms such as random forests to consider nonlinear relationships (for instance, between prepayments and interest rate variation) and loan features (for example, embedded options), as well as behavioral factors. We see five key steps:

- *Customer segmentation.* Banks can use AI to achieve granulated segmentation—for example, incorporating behavioral factors.
- *Prepayment behavior.* Banks can quantify constant prepayments and prepayments subject to criteria including interest rate levels, prepayment penalties, age of mortgage, and borrower characteristics. Leading banks establish a parent model and leverage customer segmentation to derive dedicated prepayment functions, taking into account customer protections such as statutory payment holidays.
- *Interest rate scenarios.* Banks can employ Monte Carlo simulations and other models to analyze a range of scenarios, including extreme and regulatory scenarios, and simulate potential prepayment behaviors for each scenario.
- *Hedging ratios and strategy.* Decision makers should evaluate the value of mortgages under different interest scenarios and derive sensitivities to economic value and P&L. They can then select hedging instruments with the aim of neutralizing scenario impacts.

— *Pricing.* Mortgage pricing can be adjusted based on maturity and potential prepayment behavior. Banks can use fund transfer pricing, with risks handled by a dedicated team in the treasury function.

Another important focus area is deposit decay. Many banks still prioritize moving-average approaches segmented by maturity and backed by expert judgment. A best practice would be to identify a core balance through a combined expert and statistical approach, looking at trends across customer segmentation, core balance modeling, deposit volume modeling, deposit beta and pass-through rates, and replicating portfolio/hedge strategies. This would mean leveraging AI and high-frequency data relating to transactions, to estimate each account's non-operational liquidity, which customers may be more likely to move elsewhere (see sidebar "Case study: Deposit modeling to limit deposit erosion"). Some banks also use survival models to gauge non-linearities in deposit behaviors.

In the context of IRRBB strategy, leading banks are keeping a close eye on both deposit beta and pass-through rates (the portion of a change in the benchmark rate that is passed on to the deposit rate). They back their judgments with views on client stickiness, which they traditionally arrive at through expert judgment and market research. A more advanced approach is to derive regime-based elasticities, capturing data from historical economic cycles.

Finally, risks need to be optimally matched with hedges. The recent trend is to use stochastic models to support hedging decisions, enabling banks to gauge non-linearities. Forward-looking banks increasingly integrate deposit, prepayment, and pipeline modeling directly into their hedging strategies. They also ensure model risk is closely monitored, with models recalibrated frequently to reduce reliance on expert input (see sidebar "Better modeling enables more resilience: One bank's story").

Case study: Deposit modeling to limit deposit erosion

One bank achieved an equivalent of €150 million to €200 million positive P&L impact on €30 billion of deposits by using AI techniques for repricing. The tool provided transparency on the following measures:

— the amount of liquidity at risk for each client—that is, the excess liquidity the client could potentially invest or move freely to other banks

— the churn probability for each client, or the probability the client would move the liquidity if the bank took no action, based on client sophistication, the quality and intensity of the client's relationship with the bank, and the level of market competition

— the customer value at risk, an estimate of future revenues that would be at risk if the client moved the liquidity elsewhere (for example, including not only the opportunity cost of funding, but also revenues from related services)

Armed with this transparency, the bank was able to formulate client-specific strategies for repricing actions and product offerings (for example, investment products and transaction banking services), optimizing both its funding sources and profitability. New capabilities to support the effort included a deposits command center, producing a real-time dashboard for monitoring, including early warning triggers, sales team mobilization, and new product offering, especially for cash-rich corporate clients.

Better modeling enables more resilience: One bank's story

A European global bank wanted to improve its forecasting in a rising-interest-rate context. Managers decided to focus more on customer behavior. They moved away from expert-judgment buffers to AI and stochastic modeling and a more focused approach to model calibration. They also updated scenario planning based on regulatory guidelines and best-in-class approaches, such as an "interest rate risk in the banking book" (IRRBB) dynamic balance sheet methodology. Through these changes, the bank was able to estimate its duration gap (between assets and liabilities) more accurately and thereby reduce delta economic value of equity (EVE). As a result, the bank recorded a 70-basis-point uplift in return on equity, resulting from capital savings on interest rate risk and a direct P&L impact from reduced hedging.

Enhancing Basel's interest rate risk measures: Exploring the efficacy of reverse stress testing and VAR

Research conducted by a group of bank risk managers suggests that the current supervisory outlier tests for interest rate risk in the banking book (IRRBB) may not adequately address all significant risk scenarios. Specifically, the scenarios outlined in the BCBS 368 guidelines for stress-testing economic value of equity (EVE) and net interest income (NII) may fall short in identifying substantial IRRBB risks. This oversight could make it more difficult for banks to recognize material risks of loss, especially if they have complex or unconventional portfolios.

To identify more material risks, experts are recommending a shift in approach. Instead of focusing solely on extreme and plausible scenarios, they are advised to consider all possible scenarios and integrate reverse stress testing. This would involve simulating thousands of historical and hypothetical scenarios, covering almost the entire spectrum of possible yield curves. After computing NII and EVE, attention would be directed to the scenarios that could have the most adverse impact on the bank's balance sheet.

In alignment with this proposed methodology, Australian banks will be mandated from 2025 to calculate IRRBB capital using measures of expected shortfall rather than value at risk (VAR). The change is intended to incorporate tail risk, with the new methodology utilizing data from the past seven years, coupled with a distinct one-year stress period.

Improve stress testing

Several players are integrating interest rate risk, credit spread risk, liquidity risk, and funding concentration risk in both regulatory and internal stress tests. Indeed, the IRRBB, liquidity risk, and market risk (credit spread risk in the banking book, or CSRBB) highlight the trade-off between capital and liquidity regulations. In short, higher capital requirements may reduce the need for excessive liquidity, and vice versa, for a bank with stable funding—a situation that remains a challenge to current regulatory frameworks.

Stress testing to measure interest rate risk is also evolving, with some banks adopting reverse stress testing (see sidebar "Enhancing Basel's interest rate risk measures: Exploring the efficacy of reverse stress testing and VAR").

In upgrading their stress-testing frameworks and interest rate strategies, banks need to balance net interest income (NII) and economic value of equity (EVE) risks that may materialize as a function of rate volatility. On NII, banks can productively apply scenario-based yield curve analysis across regulatory, market, and bank-specific variables and weigh these in the context of overall balance sheet exposures, hedges, and factors including deposits, prepayments, and committed credit lines. Additional economic risks include basis risk, option risk, and credit spread risk, which also should be measured.

Tailor planning

Bank funding plans are often generic, periodic, and spread across different frameworks and methodologies, including funding plans, capital plans, internal capital adequacy assessment processes (ICAAP), and internal liquidity adequacy assessment processes (ILAAP). They are often designed for a range of purposes and audiences and updated only when prompted by regulatory requirements. In future, banks will need dynamic, diversified, and granular funding plans—for example, tailored to products and regions. The plans should reflect flexible and contingent funding sources, central bank policies, and the trade-off between risks and costs.

Embrace dynamic hedging strategies

In the era of low rates, hedging of interest rate risk was a less prominent activity. Banks often employed simple, static, short-term, or isolated strategies, mostly aimed at protecting P&L. Few banks paid a great deal of attention to collateral management.

Now, in a more volatile rate environment, the potential for losses is much higher, suggesting banks need more sophisticated, agile, and frequent hedging to respond to shifts in interest rates, credit spreads, and customer deposit behaviors (Exhibit 3). Indeed, in 2023, the traded volume of euro-denominated interest rate derivatives increased by 3.4 times compared with 2020, according to the International Swaps and Derivatives Association.[3]

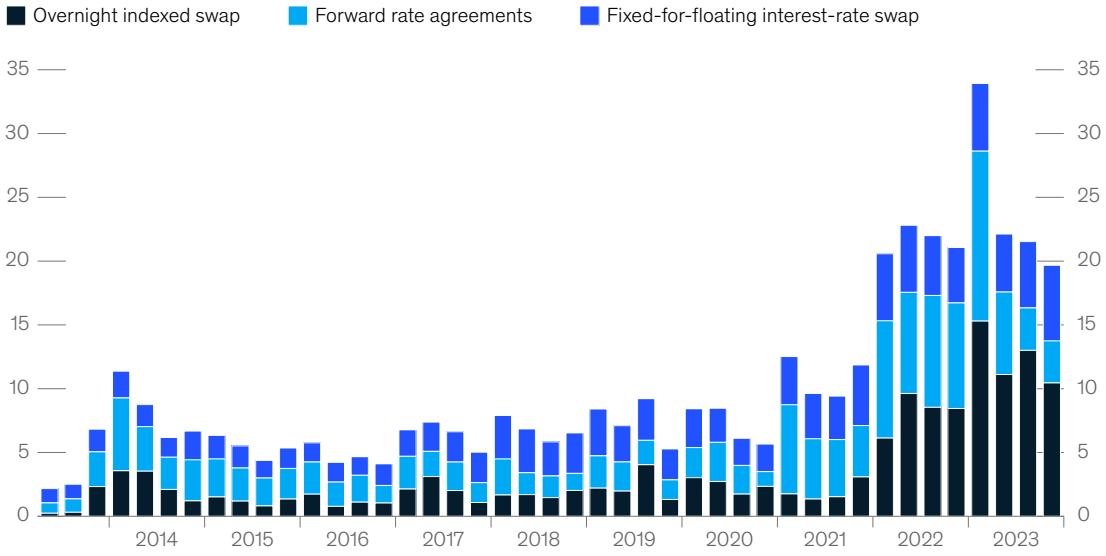
Hedging strategies are evolving to be dynamic, horizontally integrated across the organization, and wedded to risk appetite frameworks, so banks can balance P&L priorities and reductions in tail risk. On the ground, banks will likely need to recalibrate their strategies frequently, ideally leveraging a comprehensive scenario-based approach to reflect changes in the external environment. Many, for example, have already revisited hedging to reflect higher rates, but as rates fall, they will need to assess factors such as the impact of convexity on short positions. The objective of these exercises would ideally extend beyond risk mitigation to the optimization of NII (see sidebar "Replication and hedging: The upsides of NIM optimization").

[3] "Interest rate derivatives US: Transaction data," ISDA.

Exhibit 3

Banks have been more active in interest-rate hedging.

European interest-rate derivatives traded notional, quarterly,[1] $ trillion



[1]Includes all terms and all execution venues. Transactions reported by approved publication arrangements, and trading venues located in the European Union and UK. The data is displayed with a 5-week delay due to the posttrade transparency deferrals.
Source: International Swaps and Derivatives Association

McKinsey & Company

Replication and hedging: The upsides of NIM optimization

Broadly, banks may consider four approaches to replication and hedging, each of which offers benefits that will vary according to the bank's unique asset base.

Static replication is a widely applied and robust approach that involves derivation and adjustment of cash flows from deposit volume models for deposit rate elasticity and pass-through rates. The remainder of cash flows are replicated with bonds, interest rate swaps, or loans. Future deposit growth can be incorporated if desired.

Dynamic hedging of present value of net interest margin (NIM) treats the deposit portfolio like a structured product. Banks calculate the present value of NIM arising from deposits, enabling derivation of present value sensitivity to changes in interest rates. The method supports dynamic hedging and can take into account negative convexity.

Static NIM optimization provides the recommended trade-off between granularity and sophistication on the one hand and usability on the other, and it is our preferred approach. It involves design of the fixed-income portfolio to replicate deposit balance dynamics over a sample period. The analyst then selects the portfolio yielding the most stable margin, represented by minimization of margin standard deviation of the spread between the portfolio return and deposit rate. The approach enables NIM maximization, with the caveat that shorter tenors tend to be preferred in periods of low benchmark rates.

Dynamic NIM optimization permits banks to model future interest rates with NIM and investment strategy optimized for a future horizon. Again, NIM can be maximized, but the approach requires assumptions on volume growth, and the optimization horizon may not extend to the full rate cycle.

A key principle of best-in-class hedging strategy is that a proactive, forward-looking approach tends to work best and will enable banks to hedge more points on the yield curve. And with forward-looking scenario analysis, they should be able to anticipate risks more effectively. Consider the case of a bank that was exposed to falling interest rates and did not meet the regulatory threshold for outliers under the new IRRBB rules for changes in NII. Through analysis of potential client migrations to other products and a push to help clients make those transfers, combined with a new multi-billion-dollar derivative hedging strategy, the bank brought itself within the threshold.

Banks should not view hedging as a stand-alone activity but rather as integrated with risk management, backed by investment in talent and education to ensure teams choose the right hedges for the right situation. These may be traditional interest rate derivatives but equally could be options or swaptions to bring more flexibility to the hedging strategy. AI will be table stakes to support decision making and identify risks before they materialize. A more automated approach to data analytics will likely be required. And collateral management should be a core element of hedging frameworks, with analytics employed to forecast collateral valuations and needs, optimize liquidity reserves, and mitigate margin call risk.

Next steps: Making change happen

To effectively implement change across the activities highlighted here, best practice would be to bring together modeling capabilities under a dedicated data strategy. The target state should be comprehensive capabilities, a unified and actionable scenario-based framework, and routine use of AI techniques and behavioral data for

decisions around pricing and collateral. Most likely, a talent strategy also will be required to support capability building across analytics, trading, finance, pricing, and risk management.

Banks must marshal a broad range of market data to support effective modeling. The data will include all credit lines, including both on–balance sheet and off–balance sheet items, deposit lines, fixed-income assets and liabilities, capital items, and other items on the banking book. Ideally, banks would assemble 15 to 20 years of data, which would take in the previous period of rising interest rates from 2004 to 2007. Alongside these basic resources, banks need information on historical residual balances, amortization plans, optionality, currencies, indexing, counterparty information, behavioral insights, and a full set of macro data. Some cutting-edge models incorporate about 150 different features.

Armed with comprehensive data, banks can build behavioral models (for example, prepayments, deposits) to estimate parameters and infer behavioral effects in different scenarios. They can then integrate behavioral outputs into stress-testing simulations, alongside expert-based insights. Once macroeconomic data has been inputted, banks should be able to compute delta NII and EVE for three years. Visualization tools and hedging replica analysis can help teams clarify their insights and test their hedging strategies across risk factors.

Banks that have embraced the levers discussed here have set themselves on a course to more proactive and effective interest rate risk management. Through a sharper focus on high-quality data and the use of AI and scenario-based frameworks, banks have shown they can make better decisions, upgrade their hedging capabilities, optimize the cost of funding, and ensure they stay within regulatory thresholds. In short, they will be equipped to respond faster and more flexibly as interest rates enter a new era of volatility.

Andreas Bohn is a partner in McKinsey's Frankfurt office, **Sebastian Schneider** is a senior partner in the Munich office, **Enrique Briega** is a knowledge expert in the Madrid office, and **Mario Nargi** is an associate partner in the Milan office.

The authors wish to thank Gonzalo Oliveira and Stefano Terra for their contributions to this article.

McKinsey & Company | QuantumBlack AI by McKinsey

The promise of generative AI for credit customer assistance

Generative AI can enhance knowledge of the credit customer journey and lead to improved outcomes.

This article is a collaborative effort by Bruno Batista, Márta Matécsa, and Matt Higginson, with Jose Luis, Pablo Fulcheri, and Stephan Beitz, representing views from McKinsey's Risk & Resilience Practice.

With the rapid emergence of generative AI (gen AI), credit customer assistance and collection functions are taking advantage of the technology's potential. They can use it to enhance operational capabilities, improve efficiency, increase effectiveness, and—most importantly—create better outcomes for customers.

In recent years, technological disruption has been an inseparable component of credit customer assistance and collections. The shift has been driven by increasingly tech-savvy customers and transparency demands from regulators, both fueled by the COVID-19 pandemic and other credit crises. So far, these technological advancements, such as machine learning (ML) modeling, digitization, and automation, have enabled credit customer assistance and collections to become more streamlined, data driven, and customer oriented. New technology has allowed the offering of more services, more relevant arrangements with customers, new renegotiation pathways, and improved settlement conditions. These can strengthen the customer relationship with institutions, improving customers' financial health and long-term value to institutions.

Gen AI is the latest and potentially most transformative of these advancements, and it can have an unprecedented positive impact on customer assistance. It can improve and personalize customer contact, boost the capability of agents serving clients, and automate routine processes, such as note taking, interaction summarization, and even some customer interactions. In turn, these benefits can aid the regulatory process through the technology's ability to organize and synthesize information.

As a result, the adoption of gen AI in the customer assistance and collections space is by no means limited to use in reducing delinquencies. It has the potential to significantly improve customer interactions and treatment and drastically reduce collection-related costs by freeing up resources in operations while effectively addressing credit losses. This enhanced credit efficiency might enable businesses to retain collections in-house as a core capability and capture additional benefits, such as customer loyalty serving as a new source of competitiveness in managing the cost of extending credit to customers. Some early use cases are already yielding measurable results.

In our experience, organizations that deploy advanced gen AI capabilities in customer assistance and collections can achieve up to a 40 percent reduction in operational expenses and improve recoveries by about 10 percent. Additionally, collections could see up to a 30 percent increase in customer satisfaction scores, driven by the technology's ability to better identify and address customers' needs on time, helping them become debt-free more quickly.

In this article, we identify the needs of customer assistance and collections functions and discuss where gen AI can add value both to organizations and to customers. We also explain when and where gen AI can be implemented and discuss three gen AI use cases that, in our view, will dramatically change the operations for collections and customer assistance.

Challenges of customer assistance and potential of gen AI

The goal of customer assistance and collections is to support customers in overcoming financial distress while minimizing losses and keeping operational costs low—efforts that enable institutions to foster strong relationships and loyalty with their customer base. These functions must balance efficiency and effectiveness without compromising the overall portfolio risk profile and customer experience.

Collections functions are typically tasked with four main priorities:

— *Creating a positive experience in the customer journey.* This has become the core obligation of the function. That means giving relevant and meaningful financial advice, offering payment holidays when appropriate, and proactively engaging at an early stage of delinquency.

— *Managing value at risk by strategically lowering financial risk.* This priority includes identifying which intervention is needed—and when—for each customer, based on their circumstances and ability to pay.

— *Minimizing cost without compromising efficacy and experience.* This includes knowing when and how to reach out to a customer, automating time-consuming tasks such as data collection and note taking, and providing incentives for using self-serve channels.

— *Adhering to regulatory guidelines and customer duty.* Strong customer care requires sensitivity for the intensity and tone of messages, analytics-based guardrails to avoid bias and availability, and the identification and implementation of the right products to improve customers' financial outlooks.

Gen AI can be used as a powerful tool to support the overall digitization of customer assistance. It's ideal for the many customers who prefer to negotiate with a machine over having to share their difficulties with a human. Gen AI can also provide a more personalized touch in messages sent to a customer base.

We see four fundamental areas, all of which can lead to better outcomes for the customer, emerging for applying gen AI in customer assistance and collections:

— *Reducing demand for manual intervention.* Gen AI can be used at scale in analyzing call transcripts and chat interactions to identify the core issues a customer is facing, such as when customers didn't receive statements and forgot payments. By addressing these root causes proactively, institutions can reduce demand for agent intervention, improving customer experience by making interactions faster, less stressful, and personalized.

— *Gathering insights and improving operations.* Gen AI applications can be fine-tuned on specific call models and employ quality control metrics to semiautomate the continuous improvement of operations. For example, the technology can interpret screen captures of common system reports to generate insights for a call center's control desk and ultimately automate parts of this function for greater efficiency. Combined, these additions can also enable agent coaching, enhanced performance management, and early intervention in quality issues. All of this can be done at scale using the information from all client communications rather than samples, both improving customer experience and helping to reduce financial risk.

— *Supporting agents and freeing up time.* Gen AI can bolster the capabilities of case handlers in real time to improve experience and help reduce financial risk. This can range from adding a knowledge assistance tool to clarify a policy or offer eligibility to interpreting conversations and suggesting an interaction approach, tone, or product to the agent. Ultimately, this could occur through automation. In turn, such a boost can reduce or fully eliminate the need for agents to spend time manually writing post-call notes into a system, freeing up their time for cases that require a high-touch approach.

— *Automating interactions.* Gen AI can help power the next generation of chatbots, human-like interactive voice response (IVR), and even virtual agents. These tools can potentially offer increased empathy and high-quality solutions for customers while speeding up the process. Additionally, they can power hyperpersonalized messages both in these channels and in mass communications (such as emails and text messages), further improving their effectiveness and the user experience.

Gen AI implementation across credit customer assistance

Getting gen AI up and working in customer assistance isn't as simple as plugging in a computer. Customer care leaders need to be sure capabilities put in place during early development enable the efficient growth of the gen AI ecosystem (see sidebar, "Principles for implementing a generative AI customer assistance journey"). The potential benefit of an all-in approach may be tempting, but simple, small, and manageable steps better serve functions initially.

When considering the implementation road map, leaders will have to balance value creation against disruption to the business and the potential for bugs. One smart approach that players are adopting is prioritizing high-value, internal use cases. These use cases can be built in a modular way, allowing for later deployment for customers when data, regulatory, and risk constraints are lifted.

Innovative customer assistance functions are choosing gen AI use cases that can be built and implemented rapidly without the need for complicated technical investments. These use cases typically involve using ready-to-use large language models (LLMs) that require limited development efforts and have minimal risk, as they rely on public or internal data and aren't client facing. Additionally, they tackle a function's area or process that is clearly defined, not scattered, and can capture impacts such as customer call insights and quality control effectively.

Early on, these use cases shouldn't require sophisticated fine-tuning or content interpretation. Instead, they should have a limited yet clearly defined set of guardrails. For example, a gen AI use case could be for analyzing call data to identify factors contributing to successful outcomes. In this scenario, the use case is simple, manageable, and easy to measure: the low-cost ability to analyze call volume has a short implementation timeline, minimal integration expenses, and limited change management or retraining requirements.

On the midterm horizon, players are considering gen AI use cases that involve real-time output. These use cases often require more controls and security measures than less-advanced ones do, as they may involve the use of confidential customer data. However, the output of the model doesn't directly interact with customers, as it requires human intervention instead.

Principles for implementing a generative AI customer assistance journey

The following step-by-step guideline can help leaders looking to implement generative AI (gen AI) across their customer care and collections functions:

1. Ideate and develop a long list of gen AI use cases.
2. For each use case, identify impact, feasibility, and the required gen AI application, such as creating a question-and-answer document and virtual expert.
3. Prioritize gen AI use cases based on impact, feasibility, and organizational needs.
4. Agree on the highest-priority gen AI use case and start the development of a minimal viable product (MVP).
5. Refine the MVP based on user experience, then roll out and scale the MVP to the full organization.
6. Repeat steps four and five for the next use case on the priority list.

Advanced applications of gen AI typically require a larger set of unstructured data from various sources to be fine-tuned. As a result, they require more advanced testing and validation processes and are more likely to be built and deployed across different areas or functions within an organization.

The most advanced applications of gen AI will require significant development effort and investment, which often leads to implementation timelines of roughly two to three years. These use cases are typically client facing. They will require both sophisticated environments to reduce latency to acceptable levels and robust guardrails to safeguard both the data exchange and the output to customers. They might be costly using today's technology.

In the long term, to truly capture the benefits of gen AI, leaders should consider how its deployment affects the end-to-end journeys of both the customer and the customer care team. Combining different use cases has much more impact than developing individual use cases does. When coordinated, one use case can leverage another to amplify the individual impact while building on the same modular architecture.

Moving to a mature gen AI system is transformational. Each area enhanced by this innovative technology will need a revised operating model to fully capture the value generated. Adjustments will be needed for existing processes, policies, human intervention, staffing, and more.

Three concrete gen AI use cases for customer assistance

Our research shows that end-to-end transformation of a business domain such as collections with gen AI use cases involving augmentation, automation, and demand reduction can yield up to 30 percent productivity gains. Customer assistance functions across institutions around the world are already implementing gen AI. Here are three examples of how gen AI has enhanced the process. These examples come with the caveat that capturing the full potential of gen AI requires the deployment of a whole portfolio of use cases that integrate with one another.

Gen AI as a low-cost, high-value performance booster

Gen AI can be used to quickly analyze unstructured data to generate actionable insights. The most intuitive application of this in the customer assistance space is to analyze call recordings for comparison of interaction quality against a proprietary knowledge base of a call model. The comparison should include objection management and empathetic approaches, among other measurements.

With minimal development or integration effort, this capability allows institutions to improve strategy and performance management by applying insights from specific calls. It can be used to improve coaching conversations by automating part of the process through self-guided dashboards, suggestions, and training programs. Gen AI algorithms can also identify patterns and use them to help leaders rethink their institution's existing strategy and call-model approach.

A consumer finance institution deployed gen AI to improve the effectiveness of its frontline customer assistance workforce. It was able to quickly identify the specific call model elements that helped keep arrangements intact, all with limited model fine-tuning. The company also used this information to create a 360-degree, personalized, digital performance management dashboard. The dashboard included call-level feedback for supervisors to use when providing coaching and personalized training, leading to a 10 percent improvement in performance.

Similarly, a major European credit manager company used the gen AI capability of natural language processing with traditional ML techniques to help identify collateral and match it to accounts. They also created a personalized digital performance-management dashboard with call-level feedback for supervisors to provide coaching and personalize training, leading to a 10 percent increase in payments.

Gen AI as a live copilot: Expanding frontline reach with real-time integration

Gen AI can serve as a copilot to boost the performance of agents in real time throughout customer conversations (exhibit). This enables a better overall customer experience through more structured and targeted interactions that focus on what matters to the customer.

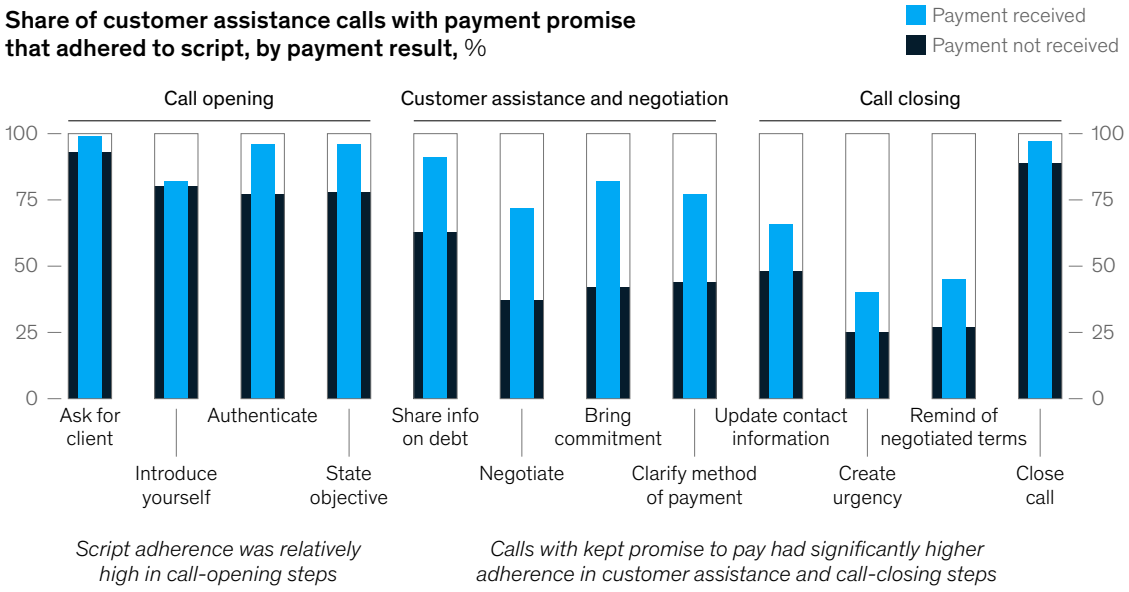
In early versions of this deployment, agents can ask a chat interface to provide a summary of previous interactions with a customer, how to respond to a specific question, and if a specific product or discount is available to an account. More advanced deployments can be integrated into telephone calls or other electronic discussions to suggest actions, products, or approaches to the agent during the evolving conversation. They can also include automatically identifying if a conversation is going outside policy, gauging quality control, and triggering the intervention of a supervisor to prevent a negative customer experience before it escalates.

For chat-based interactions, gen AI can prepopulate suggested responses for customer replies, with agents editing as needed, thus increasing the efficiency of the interaction. These conversational responses can be personalized based on customer profile, previous interactions, and current exchange to enhance customer experience and the likelihood of a positive outcome.

An implementation of this use case by a bank resulted in an estimated agent productivity increase of up to 14 percent. Using gen AI as a copilot enabled agents to handle more interactions and spend less time on research and typing. We project that average handling time could be reduced by 10 percent by providing personalized and empathetic responses, resulting in less time spent on customer service. Collection agents using this capability are also likely to have more successful debt or restructuring negotiations, leading to a 6 percent increase in recoveries.

Exhibit

Gen AI can analyze customer assistance calls to improve outcomes.



Source: GPT-4 results for 631 calls with promise to pay; McKinsey analysis

McKinsey & Company

In a simpler copilot implementation, a large bank in the United Kingdom is training existing LLMs with regulatory documentation and internal policies to provide a chatbot interface. Frontline agents will soon use it to quickly navigate product eligibility and compliance guidelines, greatly enhancing customer experience and call quality metrics. It's a step up from architecture originally developed for anti-money-laundering and know-your-customer rules.

Gen AI as a customer-facing virtual agent: Bringing full power of automation

Gen AI is already being used across industries to improve customer interactions, from restaurant drive-throughs to customer authentication in call centers. In the customer assistance space, players are looking at elements in the journey that could be automated with virtual agents to create 24/7, empathetic support to customers and free up time for real-life agents to focus on the cases that need the most attention.

The technology offers a huge benefit in efficiency. Frontline agents often spend excess time on process-heavy customer interactions, such as authenticating customers and finalizing payments that weren't completed because of technical issues. Additionally, many customers hesitate or feel uncomfortable when speaking about their financial distress to someone on the phone. Others might need to have discussions outside typical business hours.

Gen AI can alleviate much of the friction by using traditional, script-based chatbots and IVR that provide a human-like interaction experience that is both empathetic and personalized. This technology can also be integrated with existing systems to search for and provide responses to customer questions and suggest specific arrangements in real time. When the technology is stumped, it can automatically escalate to a human agent.

A utility company is currently migrating several use cases of its call center, including authenticating customers and solving specific billing issues, to a gen-AI-powered virtual agent. In this migration, the company aims to handle more than 45 percent of its inbound volumes through the new virtual agent at a fraction of the cost of customer representatives, who could then devote more time to more nuanced cases or other tasks.

Credit customer care can lead an institution's gen AI journey

The impact and benefits of implementing gen AI in the customer assistance and collection space are already being realized by fast adopters across the world. While short-term benefits can be captured immediately on specific use cases, a structured road map is necessary to capture the most value, minimize risks, and make the most out of cross-organizational investment for long-term success.

By building a scalable gen AI capability in the credit customer assistance space and coordinating with other functional areas of the organization, institutions can combine the power of data, automation, and human capital into collections that keep customers and improve finances.

The adoption of this new technology in customer assistance shouldn't be seen only as a way to quickly realize value and fund the broader adoption of the new tools. It's also a way to pressure-test an organization's capabilities and technical infrastructure needed to scale.

Integrating gen AI can improve the level of support provided to customers in financial distress in a way that can benefit everyone's bottom line.

Bruno Batista is a partner in McKinsey's São Paulo office, where **Jose Luis** is a consultant; **Márta Matécsa** is a partner in the Budapest office; **Matt Higginson** is a partner in the Boston office; **Pablo Fulcheri** is an associate partner and a senior knowledge expert in the Charlotte office; and **Stephan Beitz** is an associate partner in the Frankfurt office.

Navigating shifting risks in the insurance industry

How insurance chief risk officers balance today's complex demands.

by Erwann Michel-Kerjan and Lorenzo Serino

Today's insurers are exposed to multiple risks, from financial risks, such as shifting interest rates, changing costs and sources of capital, and increasing claims levels due to consecutive years of significant inflation, to an array of nonfinancial risks, including extreme climate events and generative AI (gen AI). This uncertain environment has spurred leaders to be more cautious but also more innovative in a way that still supports a path to sustainable, profitable growth.

The industry is taking multiple steps to manage both financial risks and pervasive nonfinancial risks. We know this based on our ongoing conversations and work with insurers and on insights gathered in our recent industry benchmark[1] of carriers (representing over $400 billion of revenues) and at the McKinsey 5th Annual Insurance CRO Roundtable—an event attended by 25 chief risk officers (CROs) of leading life and property and casualty (P&C) insurers.

The majority of participating CROs said that they expect a slight economic downturn in the next two years and predict GDP will contract by approximately 1 percent, alongside a gradual normalization of annual inflation rates to about 2 percent. A few CROs expressed concerns over a more severe economic contraction, anticipating a GDP decrease of 3 percent or more. It's clear that capital management and balance sheet management have become even more critical for many carriers, as we further discuss below.

Beyond macroeconomic pressure, CROs are working more closely with their CEOs and boards to brace against nonfinancial threats. These leaders face growing geopolitical instability and uncertainty, rapidly evolving regulatory complexity, cyberthreats, and significant climate risk—all of which can impact their portfolios. CROs also need to establish their role in the uncharted territory of emerging technologies, including gen AI, and their exponential growth. The emphasis on nonfinancial risk management is thus gaining traction. And we are witnessing more boards expecting measurable progress across these topics to better protect the insurer and, ultimately, their shareholders and customers.

In this article, we share what insurance industry CROs identify as critical issues facing their organizations, focusing on selected priorities. We analyze the steps leaders in the field have taken to mitigate these risks and discern strategies by category—whether public, private, or mutual insurers. We then sketch a pathway forward, identifying issues early on and implementing agile and resilient systems to keep insurers not only healthy but also thriving.

How insurance CROs are approaching today's risks

Insurance risk leaders have identified several issues facing the industry and point to the strategic options they are using to mitigate these growing concerns.

Capital management is becoming an even more strategic topic due to changes in the economic and regulatory environments

While the inflation spike is less of a concern this year than it was in 2022 and 2023, changes to macroeconomic conditions, regulatory requirements, accounting standards, and the competitive landscape have put significant pressure on insurers' capital positions and are pushing them to strategically rethink their optimal balance sheet composition.

For P&C companies, capacity continues to be the biggest challenge. Losses from increasingly frequent and severe catastrophes, emerging exposures, and new types of risk have produced a surge in demand for insurance coverage. As always, insurers must control costs and derisk through repricing and reinsurance. In addition, sourcing alternative capital continues to play a meaningful role. The insurance-linked

[1] McKinsey's 2023 insurance risk and resilience benchmark.

securities (ILS) market grew by more than 20 percent year to year from 2022 to 2023. Catastrophe bonds alone hit an all-time high in the first two quarters of 2024.[2] Although ILS returns have been fluctuating, there are still investors willing to both look for assets that diversify their portfolios and seek attractive returns. New business models, such as public–private partnerships, present new opportunities for different capital participation models.

For life and annuity carriers, different ownership types drive different priorities. Under pressure from investors, public companies are shifting their focus toward capital-light businesses, utilizing reinsurance and other levers to optimize capital position and returns. Private-capital-backed carriers pay close attention to ownership structure and regulatory treatment based on locations that allow them to keep the growth momentum and take appropriate investment risk under specific capital regimes. Mutual companies are generally willing to accept lower returns, but they face the same pressure of having enough capital to back their policies and staying competitive and resilient under multiple shocks and market conditions.

To build resilience, carriers need to upgrade their stress-testing capabilities. While scenario planning is top of mind for carriers, applying the scenarios vary widely. In our industry benchmark, a third of insurers reported using no more than ten scenarios for risk appetite and capital requirement determination. Yet, another third reported using up to 250. In best practice, insurers are combining scenario simulation and "reverse stress testing" techniques[3] to design and run a large number—as many as 10,000—of internally consistent macroeconomic scenarios and analyze a suite of financial measures at a granular level. By identifying potential early-warning indicators, those insurers are able to analyze the impact of management actions, create transparency on the assessment, and lead to a prioritized set of decisions.

Over time, capital management for CROs will continue to evolve from a compliance and risk play to a value creation play. This could mean moving from focusing on solvency ratio and excess capital to improving transparency on capital generation and uses of capital across business units and even products.The aim is to achieve an economic return on capital given the cost of capital for the insurer while maintaining a healthy level of excess capital. This shift would require the risk function to navigate complex (and sometimes multiple) capital frameworks, establish transparency on capital positions and uses (with possible capital reallocation across units, which is always a sensitive topic for the top team), enhance risk/return measures, and refine governance for decision making.

Gen AI at scale is expected to become table stakes for carriers; building a robust, risk-proof maintenance-at-scale model supported by the right talent will be critical

At our industry roundtable, technology, advanced analytics, and gen AI topped the list of concerns for insurance CROs. The emergence of gen AI has drawn considerable interest in the insurance world, as it does in banking, since it is viewed as both a disrupting force to the traditional business model and a powerful tool in the arsenal of underwriters, claims managers, and distribution leaders. Some insurers are considering its potential to transform distribution across life and P&C lines for both individual and commercial clients. The technology can help insurers understand the in-depth risk profiles of clients and produce much more tailored insurance contracts that suit their needs.

In a sector still defined by a high degree of manual processes and legacy systems, we expect a 10 to 30 percent increase in productivity across the risk and compliance function in insurance by deploying gen AI. Gen AI can enhance decision making by businesses by summarizing sets of documentation, improving the quality of policy information, and automating data extraction and operations.

[2] With nearly $50 billion in catastrophe bonds and insurance-linked-securties risk capital outstanding as of May 2024, according to Artemis data.

[3] As a complement to the more traditional approaches consisting of using deterministic scenarios to stress test a given portfolio, reverse stress testing to determine what multivariate scenarios would seriously impact the firm by generating tens of thousands of scenarios and quantifying interdependencies for less commonly understood scenarios as well.

A key opportunity presented by gen AI lies in addressing unstructured data. Despite strategic investments in analytics, carriers are acknowledging that data quality remains a core challenge for many of them. More than one-third of carriers in our benchmark indicated limited accuracy in maintaining a single source of truth for data.

At the same time, gen AI is also a risk that CROs and their teams will need to learn to manage in the second line of defense. The technology can present problems such as impaired fairness, intellectual property and privacy concerns, and security threats. As gen AI maturity evolves, the shortcomings of first-generation tools will be gradually addressed, especially privacy and fairness considerations.

Given gen AI's relatively novel risk profile and extremely rapid pace of development, carriers need to adapt their approach to fully integrate a transparent, responsible use of AI. In practical terms, this means establishing responsible gen AI principles and ethical guardrails, such as always having a human in the loop or restricting the use of gen AI for recruitment. Insurers must also establish risk ownership for each AI use case to ensure robust governance of AI implementation and conduct regular risk assessments to analyze emerging gen AI risk trends. Making sure the risk and compliance, as well as legal, functions are integrated early on in the development and use of these new models is key.

The industry is also facing difficulties finding the right talent to address data and technology risk management. Nearly 60 percent of respondents in our benchmark reported that data and technology risk has been the most challenging area for attracting talent. This shortage of skilled personnel in the industry poses a hindrance to fully capitalizing on the opportunity of advanced analytics and gen AI. In our experience, companies must train the teams they have but be clear about the gen-AI-specific skills they need.

We offer one more consideration. Managing the potential risks of a dozen independent gen AI models in limited use (that is, proofs of concept), which is where most of the industry is today, is one thing. But having to maintain and manage risks with hundreds of gen AI models connected with one another across the organization and hundreds or thousands of external vendors will be a daunting proposition. Many insurers are not ready for it yet; it is a capability that needs to be built.

Given gen AI's relatively novel risk profile and extremely rapid pace of development, carriers need to adapt their approach to fully integrate a transparent, responsible use of AI.

Advanced climate risk management capabilities are becoming critical competitive differentiators

When adequately priced, insurance plays an important market-signal role regarding the inherent risks being insured. The rapidly evolving climate risk landscape—events such as wildfires, extreme heat, massive flooding, convective storms, and hurricanes—and the resulting tension between conditions of insurability and insurance affordability becomes more central for P&C carriers.

From 1980 to 2010, the United States faced an average of five severe natural catastrophic events (having an inflation-adjusted $1 billion in damages or more) annually. Between 2011 and 2022, that number had tripled to an average of 15 per year, according to data collected by the US National Oceanic and Atmospheric Administration. Twenty-eight such events occured in 2023. Insurance plays a critical role in helping insured disaster victims and affected areas recover faster. The weight of these mounting claims is pressuring underwriting profitability, reserve adequacy, and ultimately, the bottom lines of these P&C carriers. Their reinsurers have also often increased the retention (the level at which they will start reinsuring), leaving many insurers with retaining a more significant portion of the losses, especially for midsize events. All of this combined is forcing even the most sophisticated market leaders to fundamentally restructure their models, increase premiums, and shrink their exposure in certain areas, or even stop providing coverage altogether as several of them have recently done in California and Florida. At the same time, the nonadmitted property market in the United States is growing 20 percent annually, as customers are increasingly forced to pursue higher-cost, nonstandard property coverage.

With mounting natural catastrophes and scientific forecasts for a continued upward trend, investors and regulators are increasingly demanding that insurers better understand their climate risk exposures and be ready for nonlinear, abrupt changes in climate patterns. For carriers with significant commercial or personal-property positions, investments in advanced climate analytics are becoming required capabilities, especially in combination with access to third-party data.

Life carriers are not immune to the climate risk conundrum. As large institutional investors, insurers are working to understand the impact of climate risk on their investment portfolios and liabilities. This is a result of recent climate risk disclosure rules, including those most recently adopted by the US Securities and Exchange Commission (SEC). On the asset side, transition risk, where changing economic conditions, market, and regulatory risks arise from the transition to a low-carbon economy, and physical risk, can fundamentally shift expected long-term returns in specific industries and asset classes.

The climate crisis is also influencing liabilities, affecting the longevity and health of policyholders. As shifting weather patterns and environmental factors impact public health, life carriers are considering the long-term effects on mortality rates, medical costs, and overall portfolio risk exposure. Carriers now face the complex challenge of factoring climate-induced health vulnerabilities into their actuarial models.

Overall, 60 percent of carriers in our latest industry benchmark reported accelerating efforts on climate risk management. The next generation of analytical capabilities is needed for insurers to integrate climate risk into organizational strategy. However, most insurers recognize that there is significant room for their climate analytical capabilities to mature: only one out of five carriers reported that they are able to quantify climate risks to the extent they would like to or have developed a forward-looking climate strategy to address climate risk exposure holistically for the organization. Boards are also getting heavily involved in the topic, with about half of carriers in our benchmark reporting having board oversight for climate risk, such as a sustainability committee. More frequent disasters, combined with new regulations, will only reinforce this trend.

Managing cyber risk is becoming a strategic priority for the second line, drawing significant investment and requiring strict prioritization

Insurers are also facing increased cyber risk exposure, as threats increase in sophistication and frequency. Insurers have access to large amounts of sensitive data that need protection. Among them are health and medical records, lists of insured items and properties, and wealth and assets under management. Even sophisticated, large carriers with significant investments in cybersecurity are not immune to such threats, with CrowdStrike reporting[4] a 75 percent increase in cloud environment intrusions and Verizon reporting[5] a 180 percent increase in breaches resulting from vulnerability exploitation. In addition, new cyberthreats are emerging, especially in connection with gen AI, and costs of cyberattacks are on the rise because of increasing fines, business losses, and remediation costs and often have significant reputational impact as well.

In this environment, cybersecurity is not only mandated by regulation; it is a core business requirement. Consumers and business partners are demanding that carriers put in place robust cybersecurity practices. At the same time, we see greater reporting requirements due to increased scrutiny from a variety of stakeholders, including the SEC's cybersecurity requirements. All major insurers have elevated cyber risk to the board level, with 50 percent of carriers discussing it quarterly.

Third-party cyber risk management, in particular, faces increased attention today. Carriers are called to examine who the core third parties are, and what their cyber risk levels are. For instance, do they process critical data or run a critical business process? Additionally, investors and regulators want to know if the carrier has additional concentration risk, and what a third party's software "bill of materials" is, such as a list of components that make up software components.

Carriers are expected to stay up to date with the latest developments in cyber technology and services, improving the organization's cybersecurity posture while also reducing spending. Many of them use so-called zero trust architecture that shifts their cyber operating model to require strict identity verification. The majority of insurance CROs we work with take a proactive stance in monitoring and mitigating cyber risk in conjunction with the chief information security officer (CISO). However, about half of the carriers in our benchmark acknowledge that cyber expertise in the risk and compliance function is relatively new, as they are now building their cyber capabilities to oversee their CISO function. Investing in targeted capabilities that are truly second line and do not repeat what the first line is already doing will be accretive.

The key to success for carriers in the second line of defense—that is, efficient and effective oversight—is conducting targeted reviews based on cyber risk scenarios and on triggers for risk threats that are based on "cyber risk appetite." To address resource constraints, the risk team should understand key risks facing the carrier, credibly challenge internal policies, procedures, objectives, and performance, and provide the board and executive team with an independent view of the first line's program, including its testing.

Putting it together: Four moves for navigating a changing risk scenario for insurers

The aforementioned risk areas are select priorities where becoming distinctive can enhance the competitiveness and resilience of the company. To thrive in an environment of economic volatility and operating uncertainty, carriers can focus on four moves:

1. *Continue to make the risk function more efficient.* Insurers today face increasing cost pressure, which is impacting budgets for risk management, too. Among insurers with more than $10 billion in revenues in our self-reported benchmark, the mean size of the risk function was slightly more than seven full-time employees (FTEs) per 1,000 FTEs in the company. That number was lower for

[4] *2024 global threat report,* CrowdStrike, 2024.
[5] *2024 data breach investigations report,* Verizon, 2024.

compliance (three FTEs per 1,000 FTEs). This can be a pivotal time to step back and continue to improve efficiency of core processes and clarify roles and responsibilities for the first and second lines. Cost savings can then be captured by making selective investments in efficiency—analytics and automation are good examples—while reducing check-the-box exercises. And while carriers will need to balance efficiency and effectiveness of their risk and compliance functions, they must consider a long-term perspective and make sure to keep residual risks under control.

2. *Build proper identification capabilities for emerging risks.* When executives across the organization have a clear and timely view of what key risks have already manifested or are currently emerging, the organization is able to navigate volatility and uncertainty most effectively. Those risks are not siloed either, and equipping the insurers with a better understanding of their interdependencies is important. This requires having in place data-enabled risk identification capabilities and flexible tech infrastructure to collect, aggregate, and monitor risk with timely data and to link it to a transparency dashboard on risk appetite. Advanced scenario planning can help here as well.

3. *Shift risk and compliance "to the left."* Ensuring the risk and compliance functions are at the business decision table early on is key. This is especially important for emerging risks. This is a shift away from being the final reviewers and approvers—the "right" of the decision-making process—to the left of the process, where they are an integral part of the development of new products, policies or changes. This shift to the left fosters a healthy risk-based decision-making culture and, ultimately, faster execution within a given risk appetite. Leaders in these functions need to be agile and ready to innovate as a business partner, not just a pure control function.

4. *Enhance strategic agility and resilience.* In the face of uncertain economic conditions and evolving industry landscapes, insurers should prioritize enhancing their strategic agility and resilience. This involves not only preparing for known risks but also building the capacity to adapt swiftly to unforeseen challenges. Implementing flexible strategies and agile operational frameworks can empower organizations to respond dynamically to changes, whether they arise from market shifts, technological advancements, or regulatory updates.

Today, insurance industry CROs are facing multiple demands from both relatively well-known and new risks. Industry leaders are resisting short-term actions and are instead focusing on the financial and nonfinancial risks that matter most, making selective investments in capabilities such as advanced analytics and gen AI. CROs, working with the CEO, the full executive team, as well as the board's audit and risk committees, are also building proper emerging-risk identification capabilities, fostering a culture of innovation, enhancing strategic agility and resilience, and prioritizing the management of technology. All of this is in service of protecting the firm, its customers, its employees, and in the end, its shareholders.

While risks are ultimately owned by the first line of defense, the CROs—whether they have been in the seat for long or are new to the role—are playing a more strategic role than they did just five years ago. We expect this trend to accelerate.

Erwann Michel-Kerjan is a partner in McKinsey's Philadelphia office, and **Lorenzo Serino** is a partner in the New York office.

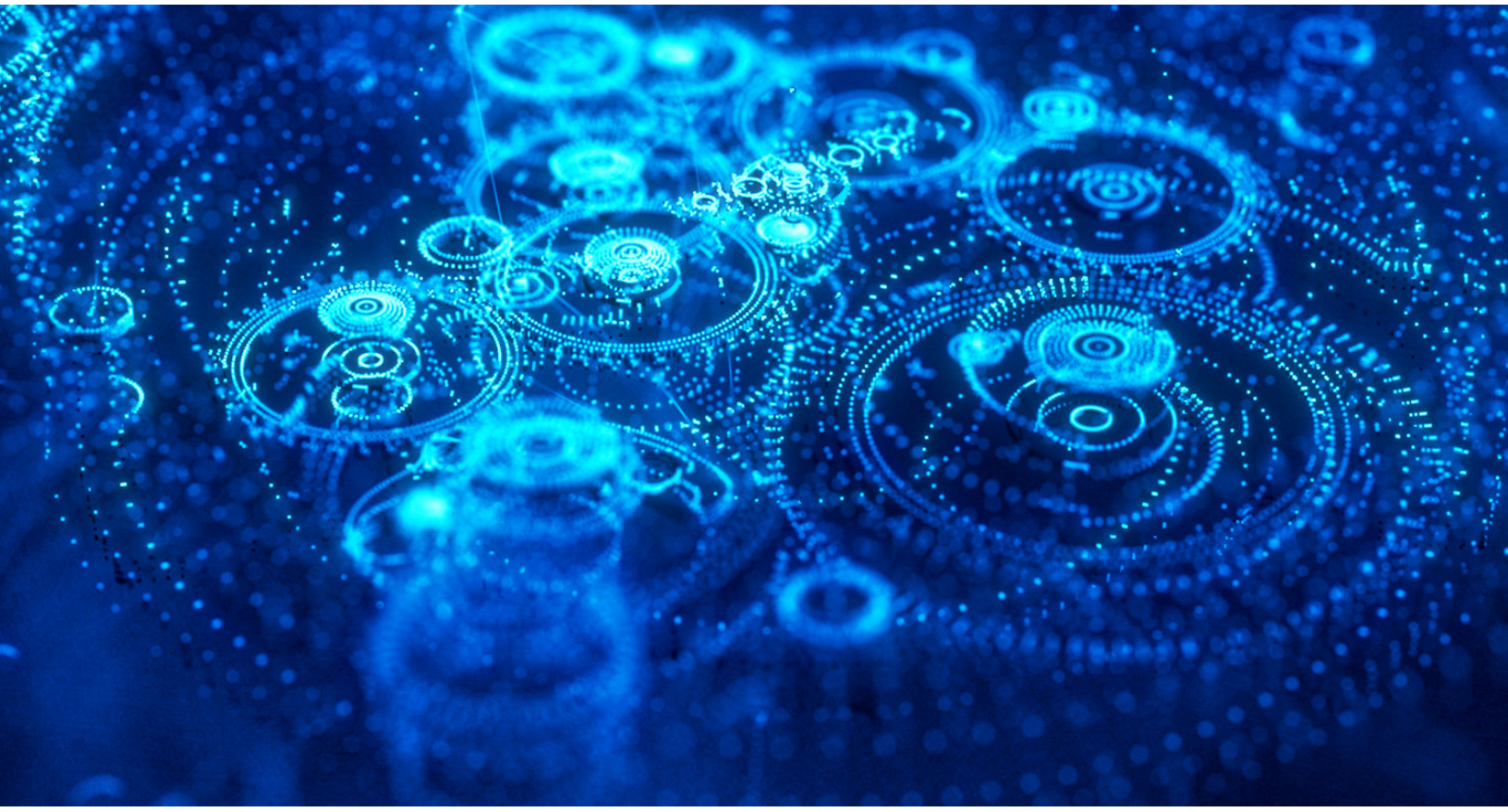
The authors wish to thank Dimitris Paterakis, Justin Greis, Liz Grennan, and Ying Zhao for their contributions to this article.

The cyber clock is ticking: Derisking emerging technologies in financial services

As financial institutions actively adopt emerging technologies, they should act now to future-proof themselves against growing cyber risks.

This article is a collaborative effort by Justin Greis, with Grace Hao, Lamont Atkins, Lauren Craig, and Soumya Banerjee, representing views from McKinsey's Risk & Resilience Practice.

This article is an executive summary of an extensive survey conducted by McKinsey & Company and the Institute of International Finance. Download the full report at McKinsey.com.



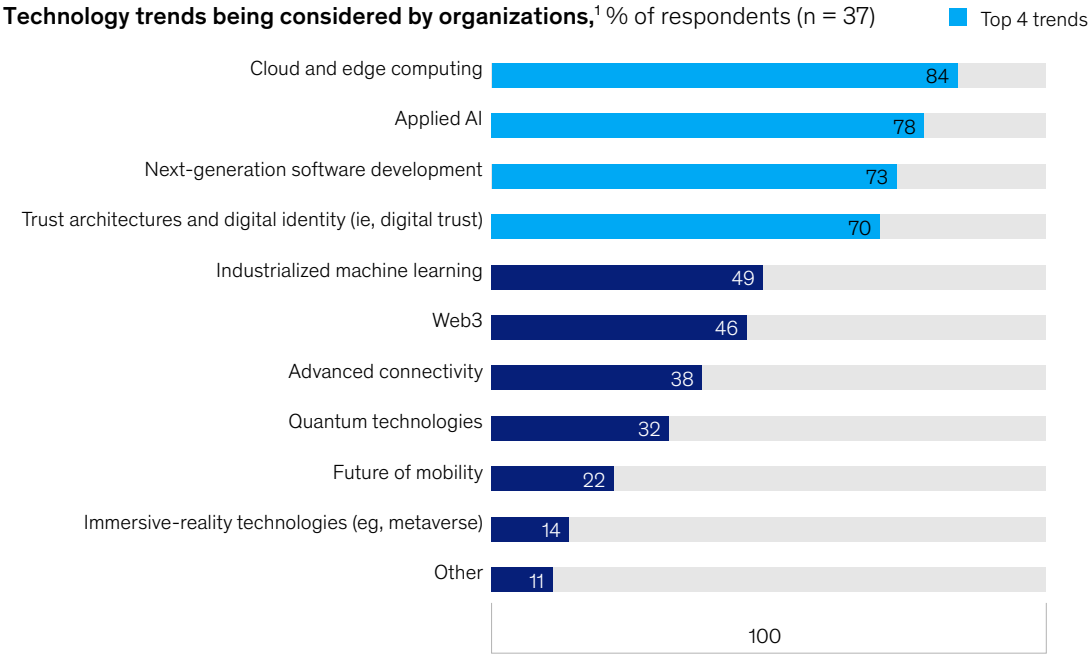
As financial-services companies around the world race to keep pace with a rapidly evolving technology landscape, they should consider not only what benefits new emerging technologies offer but also what risks they introduce.

To understand how companies are grappling with the best ways to use and protect the technologies of today and tomorrow, McKinsey partnered with the Institute of International Finance (IIF) to survey financial institutions around the world regarding their current and planned usage of ten key emerging technologies. How are companies approaching emerging technologies? What emerging technologies are they adopting? How do they plan to secure and mitigate the associated cyber risks? What cybersecurity capabilities will be needed to successfully adopt and secure new technologies?

Of the emerging technologies included in the survey (see sidebar, "Ten emerging technologies"), a majority of financial-services companies indicated that they are prioritizing adoption of and investment in four of them: cloud and edge computing, applied AI, next-gen software development, and digital identity and trust architecture (exhibit). All four technologies are likely to see quicker adoption than advanced connectivity, future mobility, immersive reality, quantum, machine learning, and Web3. This is perhaps because of their widespread applicability and maturity, as well as their proven, value-based use cases for financial-services companies.

Exhibit

Among technology trends, cloud and edge computing are applicable to most financial-services organizations, followed by applied AI.



[1]Question: Which technology trends are applicable (ie, have already been considered or discussed) to your organization?
Source: IIF; McKinsey Future of Cybersecurity Survey 2023

McKinsey & Company

Ten emerging technologies

Cloud and edge computing. In cloud and edge computing, workloads are distributed across locations, such as hyperscale remote data centers, regional centers, and local nodes, to improve latency, data-transfer costs, adherence to data sovereignty regulations, autonomy over data, and security.

Applied AI (inclusive to generative AI). Models trained in machine learning can be used to solve classification, prediction, and control problems to automate activities, add or augment capabilities and offerings, and make better decisions. Note that at the time of the development and issuing of the survey, generative AI (the next generation of applied AI, which can automate, augment, and accelerate work by tapping into unstructured mixed-modality data sets to enable the creation of new content in various forms, such as text, video, code, and even protein sequence) was included as subset of the applied AI technology category.

Next-generation software development. New software tools, including those that enable modern code deployment pipelines and automated code generation, testing, refactoring, and translation, can improve application quality and development processes.

Trust architectures and digital identity. Digital-trust technologies enable organizations to build, scale, and maintain the trust of stakeholders in the use of their data and digital-enabled products and services.

Industrialized machine learning. A rapidly evolving ecosystem of software and hardware solutions is enabling practices that accelerate and derisk the development, deployment, and maintenance of machine learning solutions.

Web3. Web3 includes platforms and applications that aim to enable shifts toward a future, decentralized internet with open standards and protocols while protecting digital-ownership rights. It's not simply cryptocurrency investments, but rather a transformative way to design software for specific purposes. This shift potentially provides users with greater ownership of their data and catalyzes new business models.

Advanced connectivity. Wireless low-power networks, 5G/6G cellular, Wi-Fi 6 and 7, low-Earth-orbit satellites, and other technologies support a host of digital solutions that can drive growth and productivity across industries today and tomorrow.

Quantum technologies. Quantum-based technologies could provide an exponential increase in computational performance for certain problems and transform communications networks by making them more secure.

Future of mobility. Mobility technologies aim to improve the efficiency and sustainability of land and air transportation of people and goods using autonomous, connected, electric, and shared solutions.

Immersive-reality technologies. Immersive-reality technologies use sensing technologies and spatial computing to help users "see the world differently" through mixed or augmented reality or "see a different world" through virtual reality.

While these technologies can provide exponential benefits, they can also bring cyber risks that companies must mitigate using their existing cybersecurity capabilities. The research shows that current capabilities are falling short of addressing these risks. Most survey respondents also recognize the need to strengthen critical cybersecurity capabilities, including third-party or supply chain management and privileged access management (PAM). As companies continue to increase their reliance on newer technologies, they must ensure they have thought through and implemented the necessary risk management capabilities. Otherwise, they may find the risks outweigh the benefits.

As the technology landscape in the financial-services industry continues to evolve rapidly over the next three to five years and as the associated risks mount, now is the time to future-proof the environment. Financial institutions can lay the foundations for action by asking themselves four questions about their pursuit of emerging technologies:

— Are we prioritizing the right technologies and cybersecurity capabilities? Are our technology priorities aligned with our security capabilities?

— Are we investing in the right technologies and cybersecurity capabilities?

— Do we have the right metrics and reporting? Can we, and do we, accurately and confidently measure against our risk appetite, provide transparency to regulators and executives, and identify strengths and weaknesses?

— Do we have the right talent to close capability gaps? Do we have sufficient and appropriate talent not just to maintain existing capabilities now but to support future maturity and technology expansions?

Justin Greis is a partner in McKinsey's Chicago office; **Grace Hao** and **Lauren Craig** are experts in the New York office; **Lamont Atkins** is a senior adviser in the Houston office; and **Soumya Banerjee** is an associate partner in the New Jersey office.

The authors wish to thank Martin Boer, a senior director for regulatory affairs for the Institute of International Finance (IIF), and Melanie Idler, an associate policy adviser for IIF.

McKinsey Risk & Resilience Practice

Global coleader and North America
Ida Kristensen
Ida_Kristensen@McKinsey.com

Global coleader and Europe
Cristina Catania
Cristina_Catania@McKinsey.com

Asia–Pacific
Akash Lal
Akash_Lal@McKinsey.com

Eastern Europe, Middle East, and North Africa
Luís Cunha
Luis_Cunha@McKinsey.com

Latin America
Elias Goraieb
Elias_Goraieb@McKinsey.com

Chair, Risk & Resilience Editorial Board
Thomas Poppensieker
Thomas_Poppensieker@McKinsey.com

Coleader, Risk Knowledge
Lorenzo Serino
Lorenzo_Serino@McKinsey.com

In this issue

July 2024
Designed by LEFF

McKinsey.com