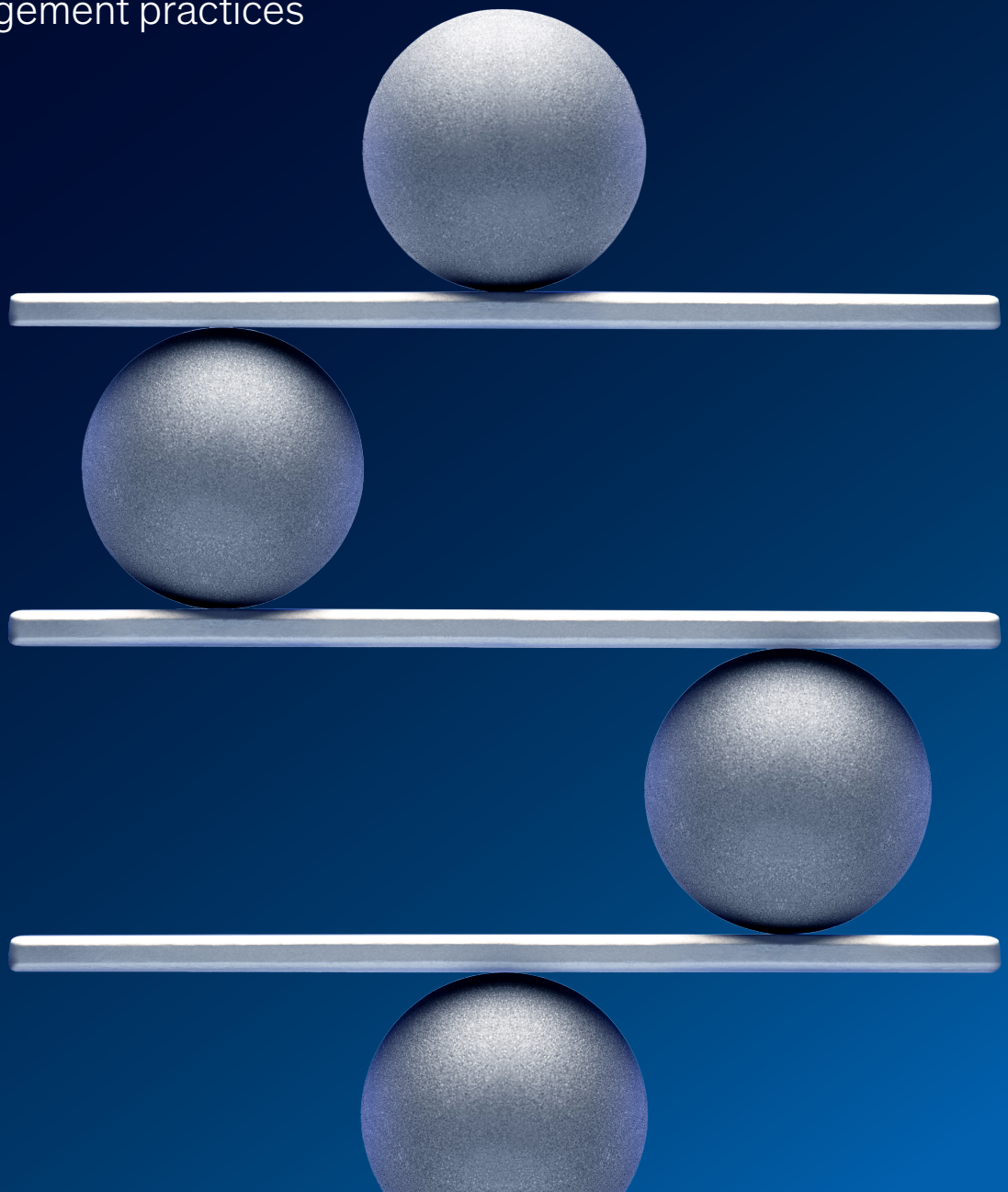
McKinsey & Company

McKinsey on Risk & Resilience

From compliance to excellence:
Elevating risk management practices



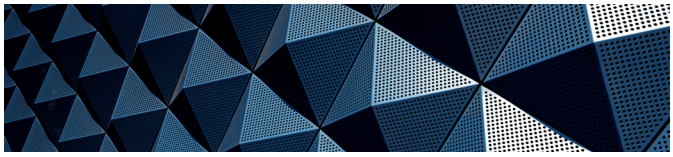
Number 18, December 2024

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:
© PM Images/Getty Images

Contents



Introduction

In this latest issue of *McKinsey on Risk & Resilience*, companies are dedicating the resources needed to move the risk management function from compliance to excellence.

Change is happening faster than ever, creating significant challenges for organizations and their risk functions. Today, leaders are unable to rely on previous experience and analysis to manage and mitigate future outcomes. Crises that before took weeks or months to develop now may happen in days or hours. No one feels these changes more than the chief risk officer (CRO), a role that was previously limited to risk but now is about building long-term resilience.

To better understand that shift, we spoke with more than 30 risk leaders from across the globe. With their experience, combined with our own insights, we identify six habits of highly successful CROs. They include being explicit about the risk and resilience purpose and vision and championing a risk-aware culture; investing in, empowering, and creating the next generation of risk—and other—leaders; leading beyond risk by engaging deeply with the executive team and board to accomplish risk and business objectives; treating supervisors as partners and being fully transparent; focusing on what only the CRO can do by integrating insights across the organization; and continually monitoring personal effectiveness and taking steps to manage time.

Our latest research and industry survey reveal that cybersecurity providers must not only rethink and innovate their products and services but also reshape how they approach customers, with the emergence of generative AI being both an opportunity and a threat.

We offer unique data and insights into the expanding and maturing role of risk in the insurance industry, in which risk management can become a strategic advantage in building business.

We discuss BCBS 239 and data risk management standards, offering five best practices for meeting these challenges and the opportunities presented.

Last, we address how AI is evolving and how the EU AI Act represents a significant step toward regulating AI systems to ensure responsible AI governance, as well as how the act could serve as a blueprint for other jurisdictions globally.

Together, our research and insights underscore the need to build maturity and excellence across the risk function, which in turn helps to drive long-term resilience across an entire organization from top to bottom.

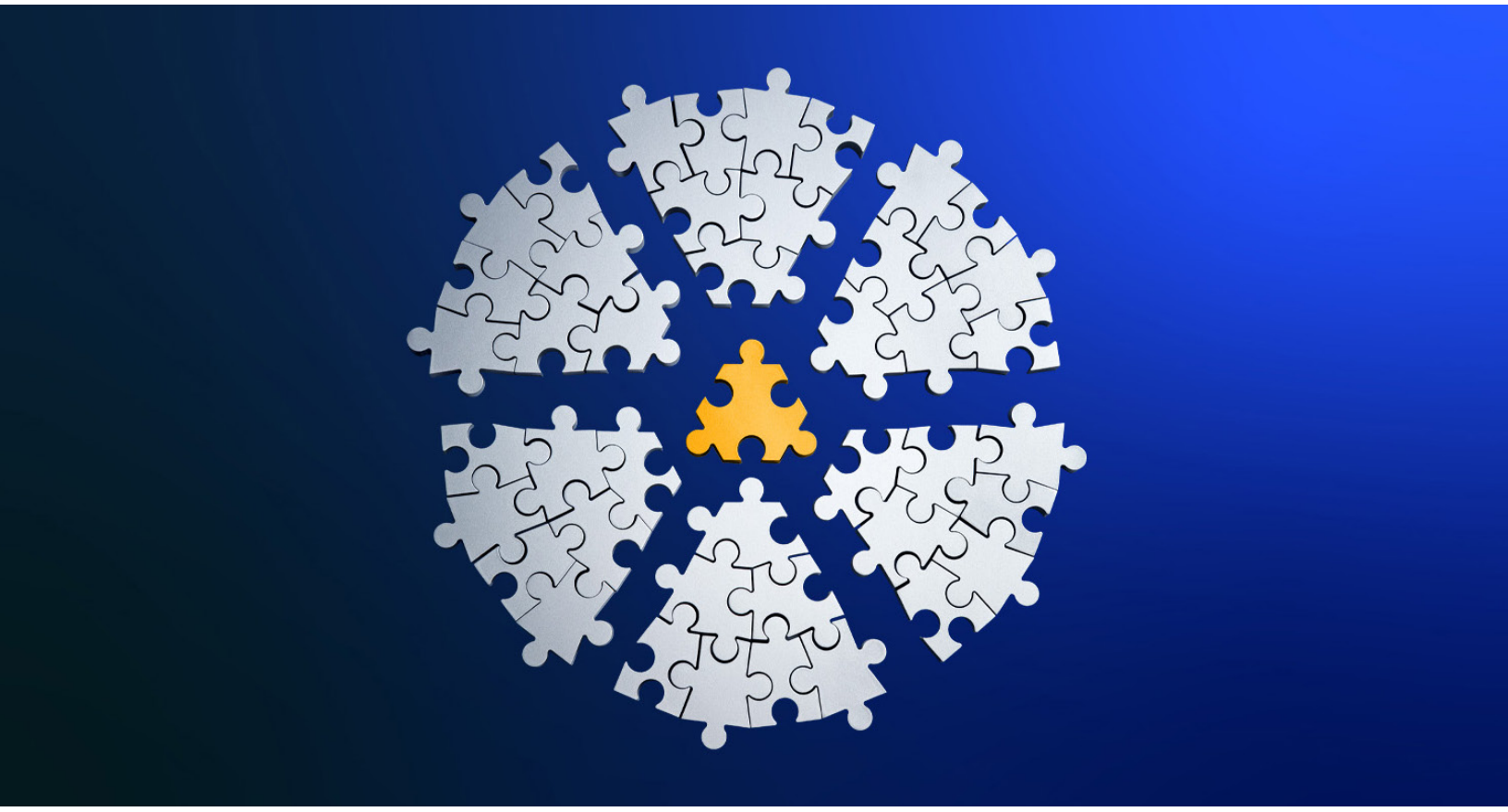
We hope you enjoy these articles and find the ideas worthy of application. Let us know what you think at McKinsey_Risk@McKinsey.com and on the McKinsey Insights app.

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

The six habits of highly successful chief risk officers

Our interviews with top CROs reveal practices risk leaders at financial institutions can use to expand their influence and build greater resilience in their organizations amid unrelenting change.

by Ida Kristensen, Marc Chiapolino, María del Mar Martínez, and Ritesh Jain



In just the past few years, a series of unprecedented and fast-moving threats have disrupted organizations. How companies, particularly financial institutions, respond to these complex risks has profound implications.

The COVID-19 pandemic wreaked havoc on credit models, and social media has played a leading role in accelerating bank runs to real time. The latter exposed a systemic risk that has required banks to rethink their liquidity and interest rate models.

No one feels these changes more than the chief risk officers (CROs) at financial institutions. Traditionally, these CROs focus on dealing with financial risk and limiting credit and market losses—both critical for keeping institutions safe for customers and the economy at large. But over time, a new era emerged in which CROs faced greater nonfinancial risk amid pressure to boost the bottom line. Today's evolving risk environment once again puts new pressures and requirements on CROs.

To be successful these days, CROs need to exert more influence and manage more risk. They need to do so amid mounting scrutiny from supervisors while building the business. Most important, they need to embed future-ready resilience in their institutions. As Richard Treagus, CRO of Old Mutual Limited told us, resilience has become the North Star guiding the CRO office and leadership suite: "We [as CROs] really need to demonstrate that organizational resilience is respected, healthy, and a high priority."

To understand just how much the CRO role is changing and which mindsets, skills, and best practices are now required for excellent risk leadership, McKinsey conducted in-depth interviews and surveyed more than 30 current and former CROs of major financial institutions worldwide; each of these individuals has spent at least five years in the role.

Through these discussions and our own insights, we identified six essential habits of successful CROs today:

1. They are *explicit about their risk and resilience purpose* and vision and champion a risk-aware culture.

2. They invest in, empower, and *create the next generation of risk–and other–leaders.*

3. They *lead beyond risk* by engaging deeply with other C-suite leaders and the board to accomplish business, resilience, and risk objectives.

4. They treat *supervisors as partners* and are fully transparent.

5. They *focus on what only the CRO can do* by integrating insights across the organization to anticipate future threats and strengthen resilience.

6. They continually *monitor their personal effectiveness* and take steps to manage time.

Many of these habits may seem familiar, but how well CROs utilize them varies. CROs told us they should be applied across all decisions. Indeed, CROs who follow these habits are more likely than their peers to manage risk more effectively and embed resilience in the organizations they lead.

> **'We [as CROs] really need to demonstrate that organizational resilience is respected, healthy, and a high priority.'**
>
> – **Richard Treagus**
> CRO, Old Mutual Limited

Habit 1: Be explicit about the risk and resilience purpose and vision and champion a risk-aware culture

Given the expanding scope of potential risks, now more than ever, employees in financial institutions' risk functions need a North Star. This guiding principle is an understanding of the organization's long-term vision, mission, and objectives relating to risk and resilience—and a risk culture to match. The most effective CROs relentlessly pursue the North Star and continually evaluate whether an organization is following it or not.

To develop this North Star, CROs will need to think beyond regulatory compliance and safeguarding the bank. While both remain essential, they are no longer sufficient as the focus for the risk function.

A good first step for CROs is to reflect on the following questions: What is the company's overarching strategy? How does our organization differentiate itself through our business model? What areas are most important to us? What do our stakeholders care most about? What does success look like? A CRO who regularly helps the risk organization answer these questions can significantly boost institutional awareness and engagement.

For some CROs, the North Star is articulated in a mission statement. One risk team used 360-degree feedback from C-suite leaders, business leads, and the risk team to come up with one. Another CRO told us his organization intentionally separated its mission statement into three sections: to set standards for the whole organization, to partner with the board and the CEO to maximize the return on capital invested in resources, and to meet regulatory and external standards (including for shareholders and communities served). Still another CRO reported that their institution's rallying cry can be summed up in one word: trust. Everything they do must reinforce customers' and employees' trust in the institution.

Getting buy-in on the value proposition can yield benefits to a risk function. A veteran CRO we spoke with said aligning values with management, shareholders, and the communities the bank serves not only demystifies risk and provides greater understanding but also helps to provide a margin for error. Stakeholders will "give you a lot of latitude to make mistakes, to manage through difficult times, if they see that your values and their values are aligned," he said.

With the vision in place, CROs can champion risk culture across the organization and foster a risk-aware culture in line with their purpose and vision. As Frank Roncey, CRO of BNP Paribas, explained, "One of my primary focuses is to preserve the risk culture of the bank, which has served us quite well so far. This doesn't mean we are necessarily conservative; it means we are disciplined, demanding, and thorough." Roncey considers himself "guardian of the temple," and his chairman sees the risk team as "angels of the bank."

"Among other things," Roncey said, "I am tasked to ensure that this culture is kept across generations. This is done through strong, principles-based risk decision making at the highest level of the organization and through clear communication about the decisions, drawing and sharing lessons from risk events or our mistakes, and explaining our decisions to younger colleagues."

One CRO would encourage transparency and timely escalation by letting his team know that "if you tell me about a risk issue and that issue subsequently blows up, then that's my problem. If you don't tell me, then it's your problem."

Establishing a mission, vision, and risk culture won't happen overnight; nor is it easy. One CRO described it as a "cultural journey" in which risk and resilience principles slowly permeate into all levels of the organization. Lorie Rupp, who has been the CRO at First Citizens BancShares since 2017, used a creative way to champion risk culture. "We found a picture of one of the teller stations in Smithfield where they had bars on the teller windows. That was risk management back in 1898. We have been managing risk as a company since the beginning of time. Then I started telling that story and everybody invited me to do that with their teams. It became a little bit of a road show to make the point that risk management is what we do every day."

Having merged risk into the organization's vision—and continually nurturing it—CROs have elevated their role. It's moved from traditional risk management to one in which a resilient culture fuels and, in many ways, leads growth. But this change doesn't happen without a team built to meet today's unprecedented changes.

Habit 2: Invest in, empower, and create the next generation of risk–and other–leaders

The demands of managing in today's increasingly complex risk environment require CROs to build a bench that meets the moment. That's why CROs create the next generation of risk leaders—and, ultimately, the organization. They do so by building a diverse team, delegating to and empowering the team, and planning for leadership development and succession from the beginning.

The CROs told us that the most critical aspect of diversity is diversity of thinking. Achieving this involves combining different backgrounds, experiences, and skill sets.

CROs also said that as nontraditional professionals learn risk, they bring their experience and point of view on board. Many leaders purposely shift workers in and out of risk and between the first and second lines of defense. In doing so, they gain a broader perspective while making external talent attraction easier. Role shifts need to happen inside the risk function as well. The same principle applies to geography. By rotating risk professionals around its geographic footprint, an organization creates opportunities for team members to share insights and adds a boots-on-the-ground perspective while also reinforcing the risk culture.

Another essential component of building a future-ready, resilient risk team is directly investing in them. CROs told us they spend an average of 34 percent of their time with members of the risk function. In this way, they get to know a team's strengths and weaknesses and its natural leaders.

For Mahesh Aditya, CRO at Santander Group, staying close to leaders in his organization during a crisis provides important insights. Aditya said that in stable times leaders often seem strong, but in a crisis, some show weakness and indecisiveness. "Do they instinctively lead or look for someone to blame . . . for me, this is the first true test of a leader," he said.

It's a process of learning and development. Many CROs told us they consistently check in with their people to give feedback. They want employees to not just accept feedback but ask for it. Successful CROs model this behavior by asking for feedback themselves. "That sets a tone of deliberate vulnerability and being open to growth, and that makes it OK for other people to do the same," said a former CRO.

Or, as former Ally Financial CRO Jason Schugel puts it, "We have some uncomfortable conversations [as a leadership team]. That's OK. But if we don't have those conversations, we won't get any better."

CROs cull top performers among junior risk professionals. They prepare them for future growth and career elevation within or outside the risk organization. Day-to-day, this can include showcasing them with an organization's executive team, business leaders, and, in some cases, the board.

As with other C-suite roles, meetings, dinners, and other events are places where CROs introduce the next wave of talent. CROs allow their top people to shine, present, and answer questions. For instance, Brian Leach initiated the Women in Risk program at Citigroup. It aims to elevate women through training and added visibility, preparing them for senior leadership roles in risk and beyond.

Handing off to junior team members can be a tall order for many CROs who feel the weight of responsibility, but as former Goldman Sachs CRO Craig Broderick said, "You don't want to be defensive of your own position; if [junior risk partners] are successful, you'll be successful." He adds, "A CRO shouldn't be insecure in that regard. For a successful organization and a successful person, there's more than enough credit to go around."

In addition to building a top team of risk professionals, the goal of developing talent is to produce a future CRO. It's not unusual for a CRO to think about succession planning on their first day on the job. At the start, there may not be an obvious candidate or front-runner, and one may not immediately emerge. Yet a CRO can nurture candidates by sharing insights and building personal relationships with the risk team.

Ultimately, these moves pay off by giving leaders the ability to delegate when necessary. Top performers take center stage and are more prepared for succession. A major part of that training will also include learning a habit that is critical to CRO excellence today: building deeper and more influential relationships with the C-suite and board.

Habit 3: Lead beyond risk by engaging deeply with the executive team and board to accomplish risk and business objectives

Today's leading CROs don't simply inform the board and the CEO; they become a vital member of the executive team and a trusted adviser to the board. They've built a deeper relationship that keeps risk and resilience synced with the organization's overall mission. They communicate early and often and generate debate, which ensures there are no surprises.

In relationship building, successful CROs are close to the board and executive team so nothing comes as a shock. CROs who see themselves as business drivers in their institutions are especially adept at this. CROs told us they spend up to 56 percent of their time with the executive team and board. Those interactions go far beyond formal meetings. Some CROs have informal talks with the CEO every day. They also talk to the board risk committee often, sometimes meeting more than once a month.

CEOs and boards always welcome good news. But CROs have an obligation to deliver uncomfortable news when needed. Having an ongoing dialogue makes hard discussions easier and fortifies the principle of "no surprises."

Relationship building, of course, requires adapting the language of risk and resilience to the language of board members. Because of diverse backgrounds, some on the board may not be fluent in the technical dialect of risk management. Some CROs see themselves as translators for the rest of the organization. They use business-focused wording instead of the risk jargon that their teams sometimes use.

Being able to cross over effortlessly into business goes beyond words. Today, CROs are more engaged with business decision making, including regarding strategy, products, markets, and M&A. They understand revenue generation and strategic priorities.

One CRO holds regular "teatime" with the organization's chief information officer (CIO). These talks help them both understand the organization's technology and information priorities, as well as the risk implications.

As some CROs put it, conversations aren't always and shouldn't always be about risk. Talking about a wide variety of issues—or what a business leader cares about—helps avoid an "us versus them" mindset as the CRO demonstrates strong interest in business development.

One of the markers of effective engagement, said one CRO, is "being called into the room when you don't need to be there and being asked to be involved in crafting a business case on day one, instead of having it handed to you for limit approvals when it is fully baked six months later. Success as a CRO is when instead of having to make outbound calls to get information and make things happen, you receive inbound calls."

The goal is to create relationships that allow for honest discussion and avoid leaders viewing challenge as criticism. "You're going to take risks, and you're going to make mistakes," Broderick said. "That's perfectly fine so long as the distribution of those mistakes and the composition of those mistakes or losses … fall within parameters and

within a spectrum that you clearly identify to the respective constituent as being possible outcomes."

Familiarity, trust, openness, and understanding are ways in which CROs have reshaped their role to make an organization more resilient. Yet these qualities aren't limited to the organization. They are needed to shift relationships with supervisors and regulators into collaborations that benefit both sides.

Habit 4: Treat supervisors as partners, and be fully transparent

Just as CROs need to understand and influence the leaders in the C-suite and boardroom, CROs should establish successful working relationships with supervisors. They should find a common ground with supervisors and try to understand their perspectives, motivations, and what makes them successful. They should also be transparent and proactive in discussing both good and bad developments.

A key to building a constructive relationship is internalizing the supervisor's priorities and understanding what problem the supervisors intend to solve.

One CRO told us they begin every conversation with a supervisor assuming they have a different view. Supervisors worry about their jobs, too. So CROs should begin by trying to understand and support the priorities of their supervisory counterparts.

A mindset of collaboration is essential. Successful CROs meet often with supervisors and openly discuss what's happening in their business. Similar to the habit of engaging the executive team and CEO, CROs should aim to avoid surprises with their supervisors. It's not uncommon among CROs today to think of supervisors as advisers on some topics.

"The important thing for any of us is to take time to understand what the regulator is trying to achieve," said National Australia Bank's (NAB's) Shaun Dooley. "We need to see them as partners, not adversaries, and take a relationship management approach with them. We have an active relationship-planning mindset internally in the way we engage with regulators." Another CRO said "You need to be transparent and collaborative, or else in the long-term you lose," adding, "We are very challenging with supervisors, but never aggressive … we try to anticipate their requests, we come very prepared, with a lot of data and facts to defend our position. For this reason, [supervisors] respect us."

Some CROs emphasize their ability to influence rule making and policy when relationships are strong and trust is established. Trust enables supervisors to lean on CROs for guidance. After all, CROs are closer to the communities that supervisors are seeking to keep safe.

Fostering stronger relationships with supervisors and regulators is one way a CRO can bring a unique skill set and value to an organization. But there's more that a CRO is especially suited to do, and the most successful make a habit of it.

Habit 5: Focus on what only the CRO can do by integrating insights across the organization

Inside the organization, successful CROs see three unique levers they can use to help their institutions succeed. First, they have a distinctive vantage point, granting them visibility and access to details across the entire organization as well as to external trends. It provides them with an independent view on cross-cutting issues with the greatest risk and resilience implications. Second, they can afford to take a longer-term vision and build resilience for future events. Finally, they are the ones managing the deployment of resources against risks that threaten the institution.

Successful CROs who engage in Habit 1—being explicit about their function's purpose and vision—have already infused risk and resilience into the organization. In turn, the business, when guided by the risk function, is always working to strengthen its resilience to make sure it is ready for any disruptions.

> ‘It’s my accountability at the top of the house to have my own independent, supported-by-facts analysis. [It’s my responsibility to offer an] extreme amount of rigor and data to give my own personal, independent view of how we’re operating within or without our risk appetite. I’m the only one who can do that.’
>
> – **Lorie Rupp**
> CRO, First Citizens BancShares

Since risk can be unpredictable in nature and timing, CROs need to build capabilities to prepare the institution for future crises that are at least partially unknown. They do so by learning from their organizations’ responses to previous crises while always looking ahead for the next potential crisis. They are ready to use those lessons not only to reduce risks but also to find opportunities that help their institutions’ business goals.

Leaders and the board may be influenced by short-term goals and pressure from investors. But the CRO is in a special—if not easy—position to help an organization find balance. As Sadia Ricke, group CRO at Standard Chartered, put it: a CRO needs to have developed “influence and gravitas” to remind leaders of the medium- and long-term impact of short-term decisions. She said, “You may, at times, not be the most liked person in the room, so you need to be prepared for this and be courageous nonetheless.” Westpac CRO Ryan Zanin said, “Even in a crisis, my demeanor is calm. That doesn’t mean I don’t have anxiety or concerns about things. But I think slowing things down initially to figure out what are the three things that we must do right away, and then what are the things that can wait until later, can enable you to run faster with confidence.”

> ‘You may, at times, not be the most liked person in the room, so you need to be prepared for this and be courageous nonetheless.’
>
> – **Sadia Ricke**
> Group CRO, Standard Chartered

Just as successful CROs make a habit of finding the right balance of their time to give to current and potential issues, they also need to manage organizational resources with the same judicious approach.

"The things that should come to me are the really big resource allocation decisions or major complex or large exposure issues or strategy for the organization," said David Kimm, former CRO of R&T Deposit Solutions. "Those are the ones I ought to be seeing, and my organization better worry about the rest."

Costs and budgets may force CROs into tough choices regarding resource management. For NAB's Dooley, reallocating resources can run afoul of a more traditional approach such as adding workers to solve a problem. "My role is to actually say, 'You know what? I'm going to disinvest in this part of the risk function because we're going to automate, and we're going to invest here. And you all might not see that as the most important priority, but I do, and here's why.'"

The habit of embracing what only a CRO can do means using a holistic view to "see around the corner" and make tough decisions. CROs need to learn from past crises, anticipate the next crisis, delegate responsibility to a trusted team, and manage resources—and their own time. Given all the new responsibilities CROs are taking on, they need to employ a final habit that keeps them balanced and ready.

Habit 6: Continually monitor personal effectiveness and take steps to manage time

Successful CROs also reflect on their own effectiveness. They are relentless and deliberate about how they spend their time, set goals, and prioritize. They maintain poise by identifying strategies to maintain work–life balance and their own long-term sustainability. These CROs recognize that running a risk function is a marathon, with occasional sprints. They ask for others' opinions, regularly meeting with industry peers while developing an inner circle of close advisers they use to stay grounded and up to date.

Many CROs highlighted what they see as a paradox of the role. It's one of the most interesting roles of their career, given its broad cross-cutting perspective on the institution. Yet it's one of the most challenging, due to the vast range of issues to handle and the various demands of stakeholders.

How a CRO manages their time and resources goes beyond personal effectiveness. Being a role model is paramount. How a CRO balances work and life and sets boundaries around each is important to motivating a team—and themselves. So input from family and friends isn't ignored. Many successful CROs have what they call a "circle of trust" that allows for honest feedback.

This includes people inside the organization who feel free to discuss a CRO's performance, as well as outside voices. CROs say the more voices the better when trying to gauge their overall effectiveness.

And yet for all the value of close advisers, CROs need time alone to read and think strategically. They need to know about current issues, meet with people in the industry, go to conferences, and participate in think tanks.

To benefit from these perspectives without becoming overwhelmed, CROs need to delegate and manage time, not only for their teams but for themselves. CROs spend different amounts of time on daily risk issues. But all of them have spent at least a fifth of their time–29 percent on average—finding and preparing for potential risks. Some spend as much as 73 percent of their time on future threats, according to our survey.

> ‘[My mother’s wisdom was] any time you do something, always think about what it will look like six months later. . . . If that means doing something that gets you fired, at least . . . you will be able to say it was because you disagreed with the principle and not because you sold yourself.’
>
> – **Mahesh Aditya**
> CRO, Santander Group

One CRO told us that after getting feedback, they adjusted their work schedule to model better balance for their team—and themselves. Another said effectively prioritizing responsibilities can include simple measures such as cutting one-hour meetings to half an hour. And many mentioned receiving encouragement from their spouses and slotting exercise into their daily routines.

For all successful CROs, engaging in self-reflection and measuring performance are critical for the endurance necessary for the role. Input from professional and personal sources ensures that work does not impede life.

The six habits of highly successful CROs—being explicit about and championing the risk and resilience purpose, investing in the next generation of leadership, leading beyond risk, partnering with supervisors, focusing on their unique role, and continuously improving their effectiveness—are essential practices that enable them to meet the challenge of today’s unprecedented risks.

Ultimately, these habits stem from the acute need for resilience and are crucial for embedding a strong risk culture within the organization. By adopting these habits, CROs can evolve their roles from risk managers to influential leaders who drive the organization’s success and sustainability in an ever-changing environment.

Ida Kristensen is a senior partner in McKinsey’s New York office, where **Ritesh Jain** is a partner; **Marc Chiapolino** is a partner in the Paris office; **María del Mar Martínez** is a senior partner in the Madrid office.

This article was edited by David Weidner, a senior editor in the Bay Area office.

The cybersecurity provider's next opportunity: Making AI safer

New technology means new challenges—and new solutions—for cybersecurity providers.

by Justin Greis and Marc Sorel
with Julian Fuchs-Souchon and Soumya Banerjee

The rapid advancement of AI and generative AI (gen AI) is fundamentally transforming the cybersecurity landscape, presenting both opportunities and challenges for cybersecurity providers. As more organizations in both the private and public sectors use AI to enhance their operations, they risk inadvertently introducing new cyber-related threats. This is creating a significant and growing demand for advanced cybersecurity solutions.

AI is also being used by bad actors as a tool to fuel more sophisticated cyberattacks and increase their volume, as exemplified by the rise in AI-enhanced social engineering and the substantial financial impact of data breaches. For example, gen AI has enhanced social-engineering techniques, in which attackers generate highly realistic phishing emails or deepfakes to trick employees into sharing sensitive information or credentials. In 2023, the total cost of cybercrime had more than doubled since 2015.[1]

While companies' response time to cyber-related risks has generally decreased over the past several years, it still takes organizations an average of 73 days[2] to contain an incident, highlighting the ongoing difficulty of containing breaches. Combined with an expanding attack surface (that is, more devices and technologies that could be breached or exploited), an increase in threat actor sophistication, a lack of skilled cybersecurity workers, and a wave of new regulations, organizations are increasingly leaning on third parties to help them manage cyber risk.

Helping companies address these risks represents a significant opportunity for providers of cybersecurity solutions, but capitalizing on that opportunity requires considerable investment in innovation and new paths to market.

In addition to securing the general use of AI, using AI to help improve security is also an opportunity for cybersecurity providers. According to our research, customers say today's cybersecurity solutions often fall short of meeting demands in terms of automation, pricing, services, and other capabilities. Helping organizations manage this risk in a cost-efficient manner is a big opportunity for cybersecurity providers, but they will need to understand AI technology and embrace it within their offerings. Innovation also remains critical in traditional cybersecurity products as the market continues to evolve, requiring providers to shift their marketing strategies to meet customers where they are seeking solutions.

AI is expanding what is already a $2 trillion opportunity for cybersecurity providers. In fact, with a large and increasing number of customers wanting to shift workloads from public cloud back to private cloud,[3] organizations will incur new costs, making the capturable value for cybersecurity providers even greater.

As more organizations use AI to enhance their operations, they risk inadvertently introducing cyber-related threats. This creates a significant and growing demand for advanced cybersecurity solutions.

[1] "Why we need global rules to crack down on cybercrime," World Economic Forum, January 2, 2023.
[2] *Cost of a data breach report 2024*, IBM, 2024.
[3] Emil Sayegh, "The evolving cloud landscape: How private clouds are reshaping the tech industry," *Forbes*, November 7, 2023.

Earlier this year, McKinsey surveyed and interviewed more than 200 cyber leaders worldwide, gaining valuable insights into how the cyber market is evolving, including a deep dive into the impact of AI on cybersecurity. Below we examine trends shaping the cybersecurity market and strategic implications for cybersecurity buyers, investors, and providers.

Attacks are increasing, with or without AI

In the face of increasing—and increasingly sophisticated—cyberattacks, organizations spent approximately $200 billion on cybersecurity products and services in 2024, up from $140 billion in 2020.[4] The vended cybersecurity market is expected to grow 12.4 percent annually between 2024 and 2027, outstripping historical levels of growth as organizations look to quell threats. At the same time, organizations are gradually spending more on third-party products than internal labor; about 65 percent of cyber budgets today represent third-party spending, and only 35 percent represent internal labor (Exhibit 1).

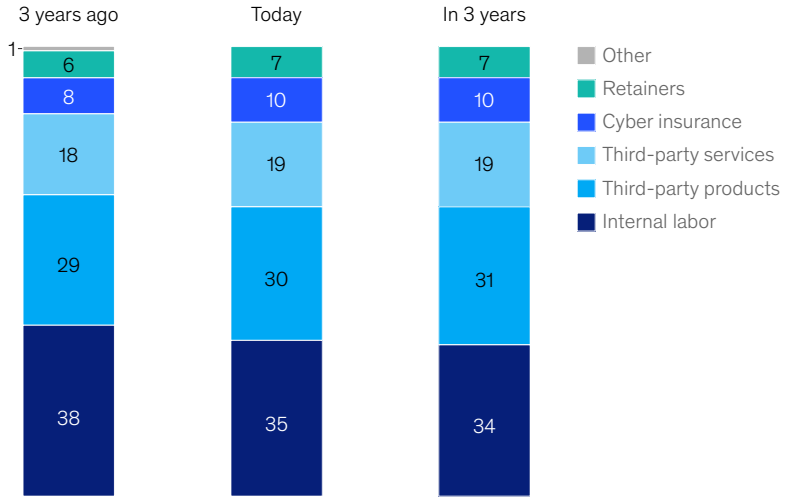
Put another way, there is a trend toward bigger budgets and spending on third-party vendors. This is driven not only by the rising number of breaches but by the cost of complying with newly introduced, strict regulations such as the Securities and Exchange Commission's rules in the United States[5] and the NIS 2 Directive in the European Union.

Organizations can harness the power of AI to help keep pace with attackers. Top cybersecurity providers are already using AI, with 17 of the top 32 cyber suppliers now offering advanced-AI use cases. However, established vendors are not the only ones introducing AI solutions. Investment

Exhibit 1

Companies spend more of their cybersecurity budgets on third-party products and services than they do on internal labor.

Average cybersecurity spending, by type, 2024, % of total cybersecurity budget



Note: Figures may not sum to 100%, because of rounding.
Source: McKinsey Cyber Market Survey, Mar 2024 (n = 200)

McKinsey & Company

[4] McKinsey Cyber Market Survey, March 2024.
[5] "Cybersecurity risk management, strategy, governance, and incident disclosure," US Securities and Exchange Commission, 2023.

in AI-powered cybersecurity start-ups has surged, particularly for application security and data protection start-ups. More than 70 percent of cybersecurity buyers at large organizations across most industries are “highly willing” to invest in AI-enabled cybersecurity tooling, though enthusiasm to adopt differs by industry. Customers are also looking not only to enhance cybersecurity capabilities with AI but also to secure other AI use cases within their organizations.

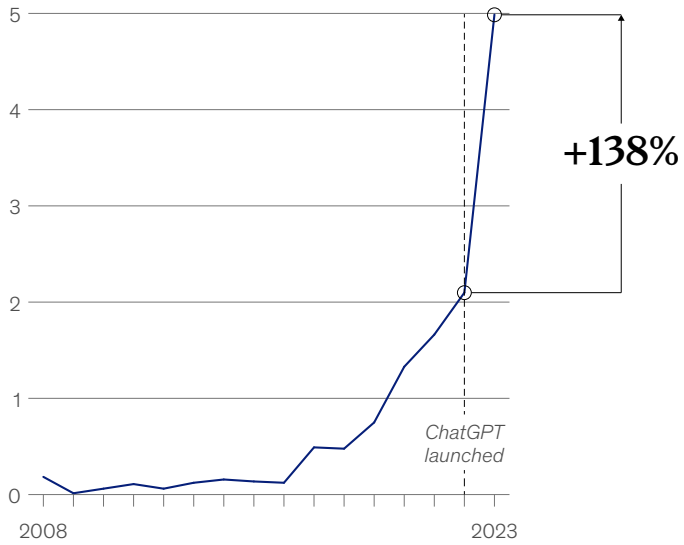
A growing attack surface is leading to higher risk exposure

The cybersecurity landscape today is fraught with familiar threats. Phishing, business email compromise, and stolen credentials are leading to breaches that are costing organizations an average of $5 million per successful incident. AI and gen AI have added a new level of danger to traditional attacks, making them harder to detect using traditional means. (Exhibit 2).

Exhibit 2

Cyberattackers continue to use generative AI to accelerate phishing as their primary method of attack.

Annual number of phishing sites detected, million



Source: *State of the Phish Report,* Proofpoint, 2023

McKinsey & Company

AI-enhanced advances also make it easier to exploit a growing attack surface, in turn introducing new risk exposure (Exhibit 3). AI-based attacks can target the traditional perimeter (for example, endpoints, servers), the modern perimeter (for example, identities, applications), and the expanding perimeter (for example, social media, data, collaboration tools). There is a growing number of devices, identities, and tools across perimeters, ranging from roughly 7 to 30 percent.

These attacks have already exploded in volume. Since the proliferation of gen AI platforms, starting in 2022, phishing attacks have risen by 1,265 percent. In short, bad actors have not only ramped up their ability to find vulnerabilities but also launched an unprecedented new wave of attacks.

Regulatory regimes and talent gap as key market drivers

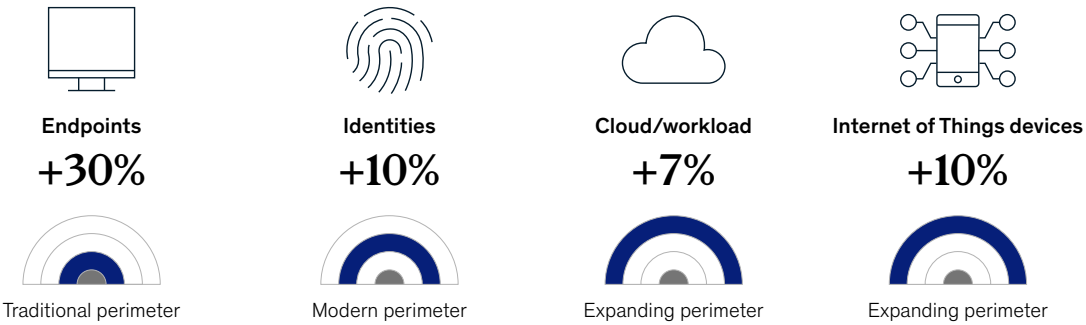
Amid this growing threat, a regulatory landscape is rapidly evolving to ensure that organizations remain resilient and are responsible stewards of customer data. Rule makers have zeroed in on secure development, data protection, reporting, and resilience. Beginning in 2023, the United States introduced several new regulatory frameworks, including Executive Order 14110[6] and CIRCIA.[7] Outside of the United States, the European Union has proposed the Cyber Resilience Act and has instituted the NIS 2 Directive and DORA[8] frameworks. To remain or achieve compliance with such regulations requires a growing cost to organizations, driving demand for cybersecurity products and services. For instance, compliance with the European Union's NIS 2 Directive is expected to increase cyber budgets by up to 22 percent in the first years following its implementation. Already, cyber regulatory risk remediation constitutes an average of more than 10 percent of cyber budgets.

The cybersecurity industry will need to fortify its talent base and resources to meet both increased threats and regulatory demands. Workers trained in cloud security, AI, and zero-trust[9] (for example,

Exhibit 3

The cyberattack surface is expanding, leading to additional risk exposure.

Expected increase in risk exposure in the next 3 years, select examples, %



Source: McKinsey Cyber Market Survey, March 2024 (n = 200)

McKinsey & Company

[6] Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023.
[7] Cyber Incident Reporting for Critical Infrastructure Act (proposed).
[8] Digital Operational Resilience Act 2022. DORA was published in the EU's Official Journal on December 27, 2022, and entered into force on January 16, 2023. It will apply in full on January 17, 2025.
[9] In this security system design, all entities—inside and outside the organization's computer network—are not trusted by default and must prove their trustworthiness.

ZTNA[10]) implementation are and will be the biggest need (Exhibit 4).

For those charged with keeping organizations safe, these new AI-based threats pose an unprecedented challenge—they are more sophisticated, unrelenting, and shifting. They are also growing exponentially.

How cybersecurity providers can capture the $2 trillion opportunity

Providers can take a series of steps to address increasing threats and seize the opportunity they present (Exhibit 5). In our work with clients and with the information collected in the survey, we have identified four clear pathways that providers can follow.

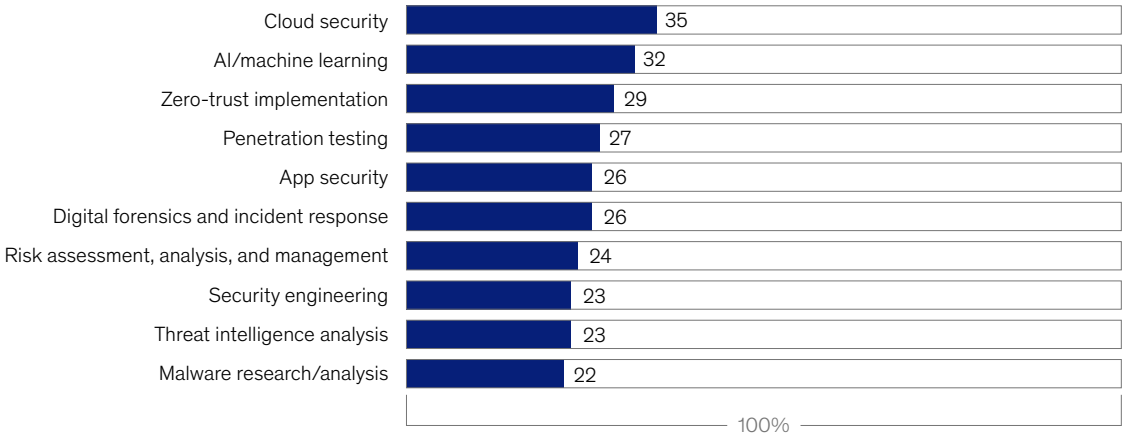
Develop AI-infused cyber products and new offerings to secure AI applications

Given the recent advancements in AI, existing cybersecurity providers are working hard to integrate AI into their existing security products. More than 90 percent of cybersecurity AI capabilities are expected to come from third-party providers.[11] As AI and gen AI have rapidly advanced during the past 12 to 18 months, most leading cyber providers have already announced AI upgrades to their existing product suite. Our survey results show that cloud security, security operations (SecOps), and endpoint security are among the market segments that will benefit the most from AI use cases. Most current AI-infused cyber products are focused on SecOps threat detection and incident response, and there are market opportunities and expectations for AI

Exhibit 4

The cybersecurity industry's biggest talent gap is in cloud security and AI/machine learning.

Share of cybersecurity professionals reporting skills gap at organization, %



Source: *Cybersecurity Workforce Study 2023,* ISC2

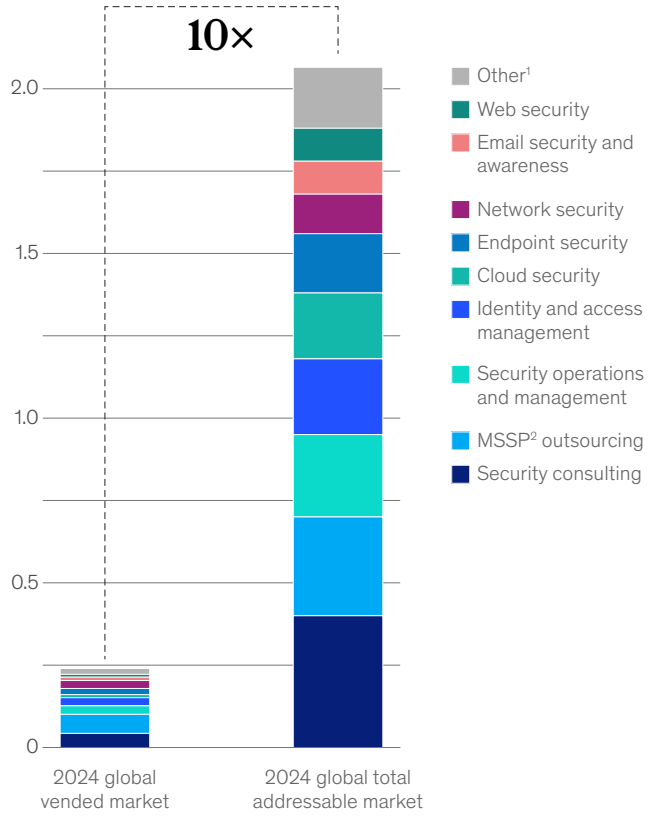
McKinsey & Company

[10] Zero Trust Network Access is a security service that allows secure access to applications, data, and services by verifying users and devices before granting access.
[11] *Securing generative AI*, IBM, 2024.

Exhibit 5

The global addressable market for cybersecurity could reach approximately $2 trillion.

Global cybersecurity market value, 2024,
$ trillion



[1]Includes governance, risk, and compliance; data protection; application security; Internet of Things; operational technology; and AI security.
[2]Managed security service provider.
Source: McKinsey Cyber Market Map, 2024

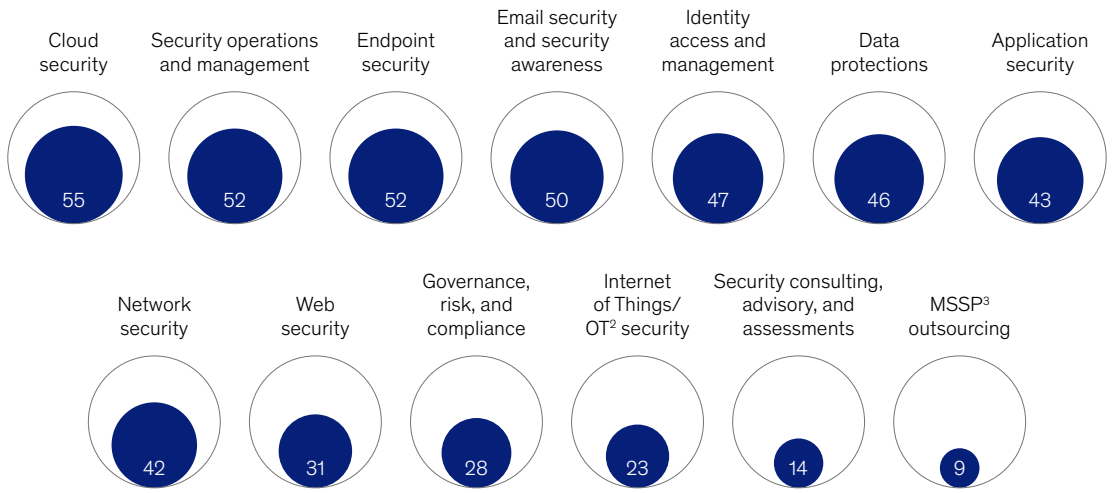
McKinsey & Company

use cases in cloud and endpoint security. Gen AI for SecOps threat detection includes suggesting and writing detection rules and queries for security information and event management by assisting in sifting through large data sets to uncover hidden threats or recommending actions to security-operations-center analysts. Providers have reported to us time savings of up to 20 to 25 percent. Also on the horizon are promising AI use cases and features such as everyday AI assistants for (nonsecurity) employees to autofill security questionnaires and reports. Providers also revealed that gen AI for autofilling security questionnaires can add time savings of up to 80 percent. For providers, the upgrades can add increased product performance and, as they will be able to increase their prices for an AI-infused product offering, a return on investment (Exhibit 6).

Exhibit 6

Generative AI is expected to significantly benefit many segments of the cybersecurity market.

Market segments that will significantly benefit from generative AI,[1] % of respondents



[1]Question: In your experience, which cybersecurity capabilities would significantly benefit from generative AI (eg, more automation through copilots, more threat detection, or faster response)?
[2]Operational technology.
[3]Managed security service provider.

McKinsey & Company

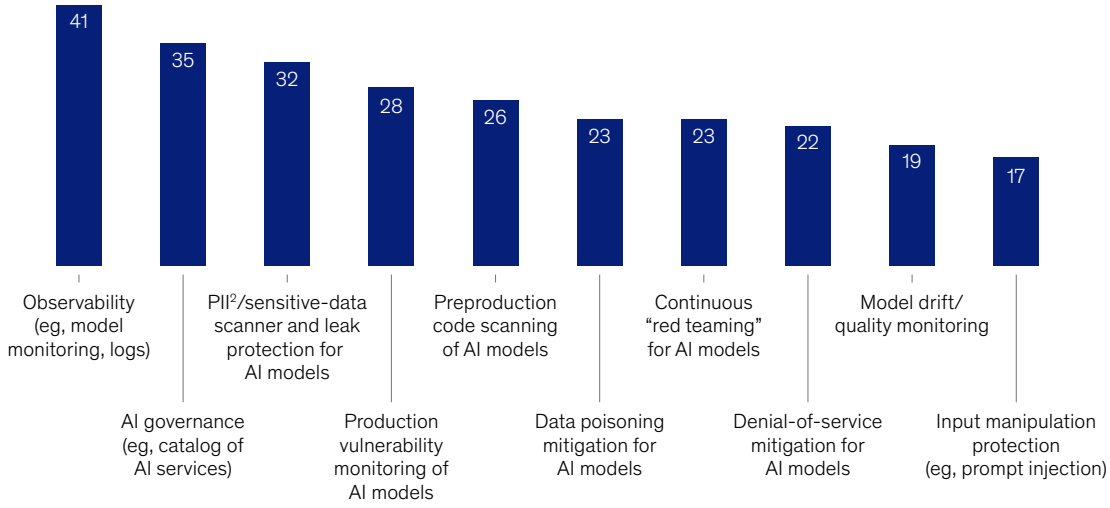
Besides the need to upgrade existing security offerings, corporations are seeking to build and integrate AI into various areas of business. Securing these new AI systems is high on the agenda for many companies. Our survey finds that vulnerability in cybersecurity is one of the top three most-cited risks of AI adoption, and many companies are prioritizing the safety of these new systems. After observability and governance, sensitive-data scanning, vulnerability monitoring, and code scanning are the top security AI use cases and will require investment. Nearly all customers (more than 97 percent) anticipate spending more on outside vendors to secure AI use cases, and 52 percent say securing AI systems will increase vendor costs by more than 5 percent (Exhibit 7). In our Cyber Market Map, securing AI is now a stand-alone cyber-market segment that is poised to grow to $255 million by 2027, from $122 million today, with a total addressable market of $10 billion to $15 billion.

Customers are looking to secure AI use cases primarily through existing vendors, but they are willing to seek out new vendors if existing vendors cannot sufficiently secure in-house AI systems.

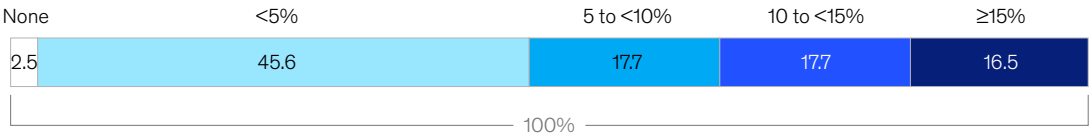
Exhibit 7

Organizations have clear needs and allocated budgets to address cybersecurity-related AI risks.

Top AI security capabilities customers are looking to adopt,[1] % of respondents selecting option as a top 3 capability



Additional third-party spend needed to secure AI use cases,[3] % of respondents



[1]Question: Which AI security capabilities is your organization looking to adopt?
[2]Personal identifiable information.
[3]Question: How much additional costs will you expect to incur to secure these AI use cases (if any)? Please answer as a % relative to existing cost of relevant vendor products/services.
Source: McKinsey Cyber Market Survey, March 2024 (n = 200)

McKinsey & Company

In short, providers that can secure AI and tailor offerings to priority customer use cases will have a competitive advantage (Exhibit 8).

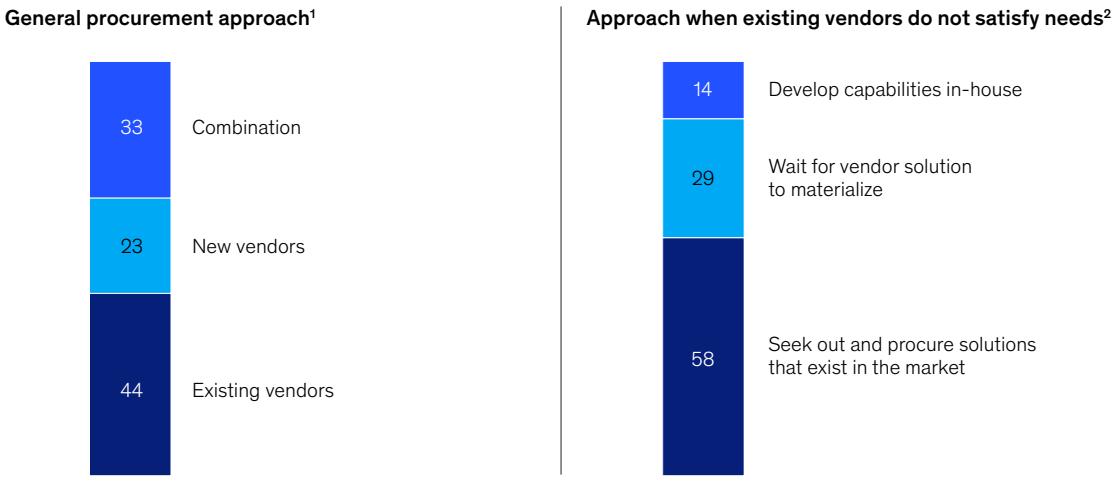
Adapt a go-to-market approach to evolving market dynamics

Evolving market dynamics are changing the way cybersecurity providers reach potential customers. Today, nearly 15 percent of cybersecurity spending comes from outside the chief information security office (CISO), and non-CISO cyber spending is expected to grow at a 24 percent CAGR over the next three years (Exhibit 9). This has changed from a decade ago, when almost all cybersecurity spending came from the CISO organization. Providers will need to increasingly cater to non-CISO customers, with most non-CISO cyber spending coming from buying centers responsible for cloud, product, network, and audit and compliance.

Exhibit 8

Customers will give current vendors first opportunity to secure AI use cases but won't wait long to seek other options if needs aren't met.

Approach to securing AI/generative AI use cases, % of respondents



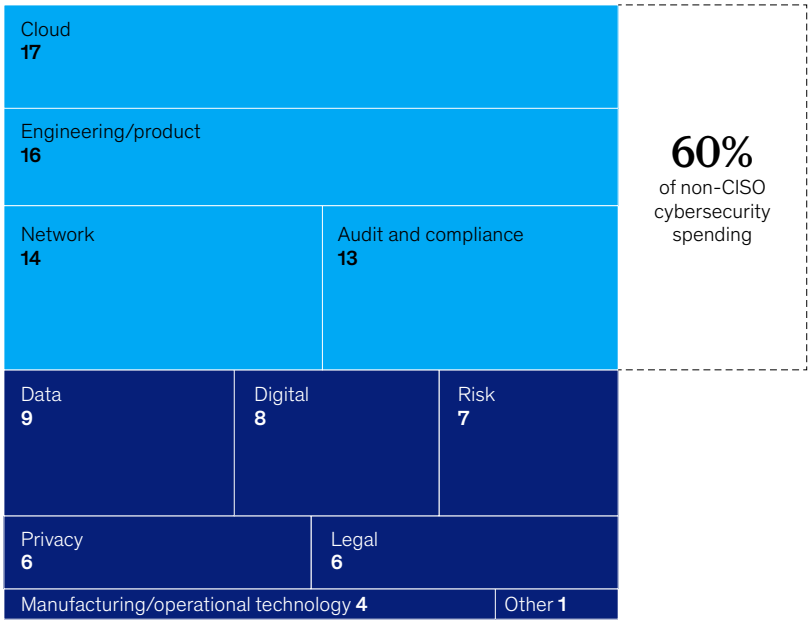
Note: Figures may not sum to 100%, because of rounding.
[1]Question: To what extent do you expect to secure AI/generative AI use cases through existing vendors vs new tools?
[2]Question: For capabilities not satisfied by existing vendors, which of the following actions are you planning to take?
Source: McKinsey Cyber Market Survey, Mar 2024 (n = 200)

McKinsey & Company

Exhibit 9

Companies are steering cybersecurity spending to outside vendors, with cloud security the biggest source of external spending.

Average source of cybersecurity spending outside chief information security office (CISO),[1] %



Note: Figures do not sum to 100%, because of rounding.
[1]Question: In your best estimation, how much of your cybersecurity spend comes from outside of your CISO organization? Where does that non-CISO cyber spend come from?
Source: McKinsey Cyber Market Survey, March 2024 (n = 200)

McKinsey & Company

Second, while most cyber sales and marketing dollars are historically spent on direct-sales and digital-sales campaigns, customers are now leaning into education and reputation to help them find providers. Customers are using industry reports, referrals, and industry analyst consultations in their decision making. They are also turning to service providers and value-added resellers when purchasing solutions.

Finally, customers that do buy cybersecurity services say improving cybersecurity maturity scores and risk ratings are big factors in their decision. These metrics are also valuable when customers want to communicate the impact to stakeholders.

Adapting the go-to-market strategy to these changing market dynamics can help companies capture a larger piece of the pie.

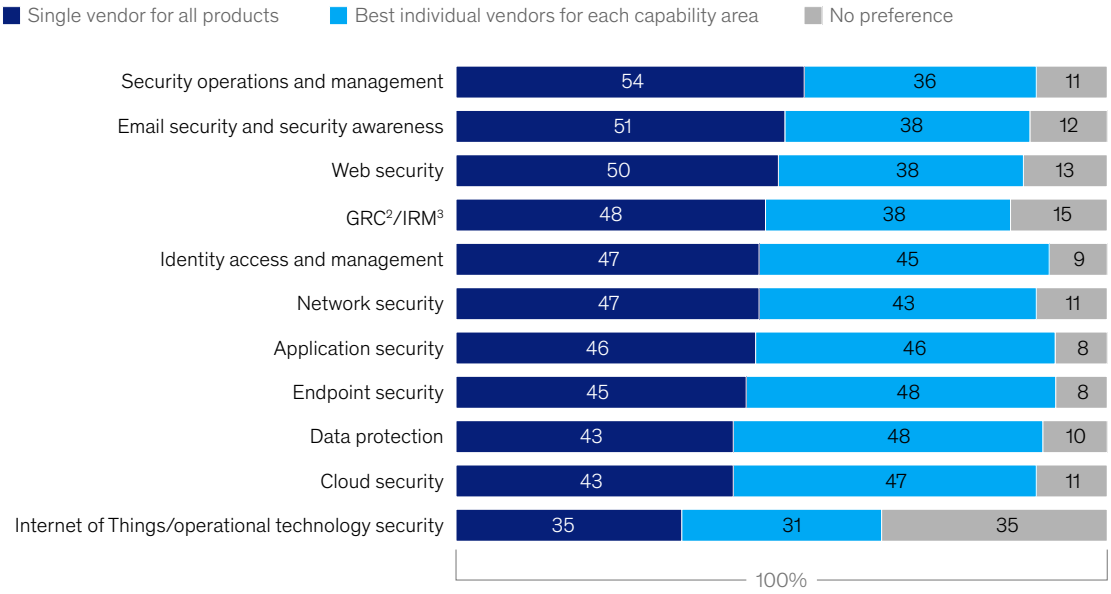
Create all-in-one offerings for highest-priority customer use cases

Our survey suggests the market is at an inflection point on best-of-breed offerings—that is, the best offering in a specific, narrow niche—versus best-of-suite offerings, which are complete, all-in-one solutions. For some segments, customers prefer the best individual vendors for each product on the market; for other segments, customers prefer to use the best product suite on the market. In practice, most customers are still using a broad array of cybersecurity products, with larger organizations using as many as 50 to 200 of them. Some are shifting to vendors that provide the biggest suites, but many still rely on best in class. Providers can therefore try to cater to both types of customers, building best-of-suite bundled offerings around standout best-of-breed offerings (Exhibit 10).

Exhibit 10

The cybersecurity market is at an inflection point on 'best of breed' vs 'best of suite.'

Cybersecurity vendor preferences, by capability,[1] % of respondents



Note: Figures may not sum to 100%, because of rounding.
[1]Question: In the future, will your company prioritize finding a single vendor for all of your products (ie, "best of suite") vs the best individual vendors for each capability area (ie, "best of breed")?
[2]Governance, risk, and compliance.
[3]Integrated risk management.
Source: McKinsey Cyber Market Survey, March 2024 (n = 200)

McKinsey & Company

For example, if a provider has a best-of-breed offering today, it can look to develop best-of-suite offerings through acquisition, the development of new products, or the bundling of existing ones. It can also look to build best-of-suite offerings through partnerships such as enterprise resource planners and customer relationship planners. Practically, providers can create these best-of-suite offerings around common cross-segment packages today.

While providers are turning to best-of-suite bundled offerings, there is also a shift toward consolidation. In three years, customers expect to use fewer vendors for network and endpoint security. At the same time, there has been a steady decline in the number of new cybersecurity companies formed since 2017, suggesting a maturing market ripe for consolidation.

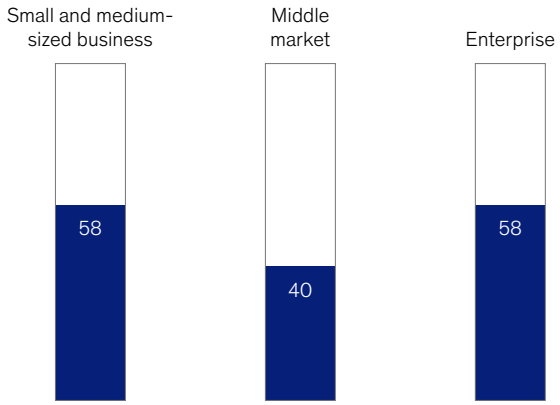
Prioritize innovation beyond AI

Beyond AI, there continues to be customer demand for innovation, especially for zero-trust capabilities. Zero-trust architecture has the potential to increase adoption rates over the next three years, with the highest potential demand in middle-market companies (Exhibit 11). Providers can increase zero-trust adoption for middle-market customers by assuaging customer concerns that legacy systems and fragmentation inhibit zero-trust adoption within a company's environment.

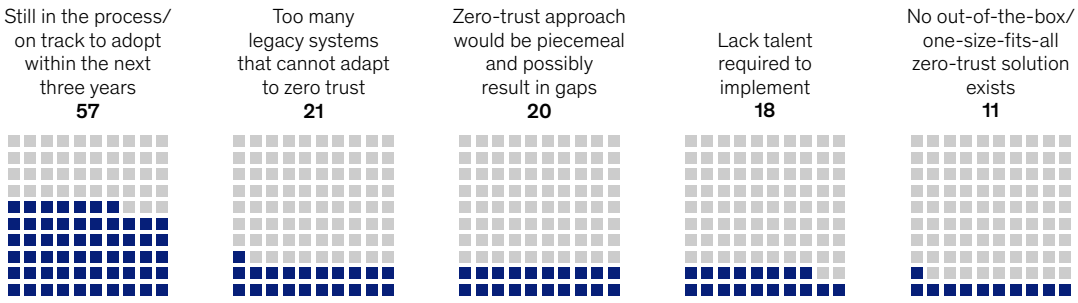
Exhibit 11

Zero-trust architecture has the potential to be more widely adopted, especially in middle-market companies.

Zero-trust architecture adoption,[1] by company size,[2] % of respondents



Top 5 reasons for not adopting zero-trust architecture,[3] % of respondents whose organization has not adopted zero-trust architecture (n = 56)



[1]Question: Do you have a zero-trust architecture today?
[2]Small and medium-sized business = <500 employees (n = 12); middle market = 500–4,999 employees (n = 52); enterprise = ≥5,000 employees (n = 48).
[3]Question: Why hasn't your organization adopted zero trust?
Source: McKinsey Cyber Market Survey, March 2024 (n = 200)

McKinsey & Company

Extended detection and response (XDR) products are also popular immediate solutions in that they provide security across all parts of an organization: endpoints, network, cloud, and more. XDR providers tend to differentiate on their telemetry, as customers look to efficient high-fidelity curated signals compared with comprehensive but tedious, resource-intensive monitoring of logs. Customers are expecting to see about a 25 percent increase in log visibility in three years, and providers that can deliver more advanced telemetry could capture a larger share of the pie. Quantum security—which refers to defense against powerful quantum-computing attacks—is seen as a more medium-term priority. While quantum is further out on the adoption curve, most industries say quantum is less than five years away from being part of their cyber budget, with software and consumer and retail the most likely to adopt. Identification of where encryption keys are stored and automated recycling of encryption keys are two promising use cases where quantum is expected to play a role.

Cyber insurance is also gaining significant momentum and attention, especially after the recent global outages. While cyber-insurance firms have significantly improved their assessment and loss ratio on cyber-insurance coverage, nearly 50 percent of companies that have cyber-insurance coverage do not feel adequately covered by it, according to the survey. There is a significant opportunity, therefore, for cyber-insurance firms to improve their insurance coverage at the right price point in the cyber market.

As the cyber market expands, providers must keep pace

Cybersecurity has always been a dynamic field of moving targets and threats. The emergence of AI and gen AI presents a new challenge for companies while also amplifying existing threats. Organizations in need of cybersecurity to meet the moment are looking to providers to help ensure that these new and fast-developing technologies are manageable and that their institutions and clients remain safe.

Just as the environment has changed, cybersecurity investors and providers need to shift as well. They must rethink and innovate their products while also reshaping their approach to reaching customers.

Providers can assuage their clients' concerns and harness the dynamic changes already taking place to grow their own businesses and positions in the marketplace. To do so, they can tailor their offerings, revise how they communicate and market themselves to customers, create products that appeal to nontraditional buyers of cybersecurity services, and, finally, keep innovating on all fronts.

Justin Greis is a partner in McKinsey's Chicago office, **Marc Sorel** is a partner in the Boston office, **Julian Fuchs** is a knowledge expert in the Stuttgart office, and **Soumya Banerjee** is an associate partner in the New Jersey office.

The authors wish to thank Anatoly Brevnov, Bharath Aiyer, Elisa Becker-Foss, Jeffrey Caso, Kevin Telford, Nick Curcio, and Wolfram Salmanian for their contributions to this report.

This article was edited by David Weidner, a senior editor in the Bay Area office.

Elevating the risk function in insurance: Building a strategic advantage

Today's rapidly developing risk landscape demands a new, more nimble approach for insurance companies to assess and respond to risks, a function inherently in their DNA.

by Diego Mattone, Luca Pancaldi, and Mina Jurisic
with Daniel Kaposztas

Today, banks use risk management to help drive strategic development for growth. This is a comprehensive approach to risk that insurers should aspire to emulate, especially as new risks are emerging more quickly and creating new challenges.

According to a 2023–24 benchmarking survey from McKinsey, leading European insurers should look to reorganize their risk functions, build out the necessary capabilities, and elevate the status of chief risk officers (CROs) within the leadership structure. This will allow them to address the rapidly changing risk landscape and position the company to use risk management as a strategic advantage.

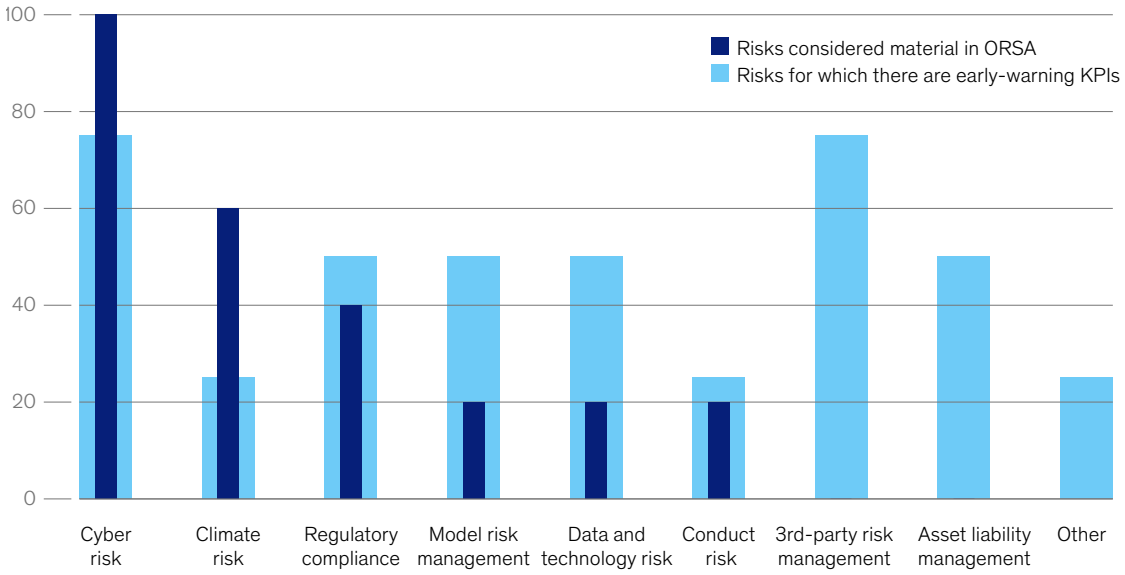
Emerging risks and challenges

One sign that risks are emerging at a rapid pace is that most insurance CROs use early-warning KPIs for a broader set of risks than those deemed material under their Own Risk and Solvency Assessment (ORSA). For example, while only 20 percent of insurers consider data and technology risks in their latest ORSA, 50 percent of CROs are using early-warning KPIs to gauge those risks. The notable exception is climate risk: 60 percent of respondents cite climate risk as material, but just 25 percent have an early-warning KPI in place (Exhibit 1).

Exhibit 1

Emerging risks already have early-warning KPIs in place, even if they are not yet included in the Own Risk and Solvency Assessment.

Which risks are considered material in the Own Risk and Solvency Assessment (ORSA),[1] and which have early-warning KPIs,[2] % of respondents



[1]Question: Which are considered material in your latest ORSA?
[2]Question: Which have early-warning KPIs?
Source: McKinsey European Insurance Risk Survey, 2023

McKinsey & Company

In fact, many emerging risks feature prominently in companies' risk taxonomies today, including data and technology, cyber, and climate risk. And, according to our survey, several challenges are adding to the complexity of the CRO task. One of the most notable is a scarcity of talent—both attracting and retaining it. Half of the survey respondents said they are having difficulty finding talent to fill roles in data and technology, cyber risk, and nonlife underwriting.

Moreover, talent problems exist to some extent in all areas of risk management (except in financial crime, according to our survey participants). This shortage of skilled personnel in the industry poses a hindrance to fully capitalizing on the opportunity of artificial intelligence and generative AI. In our experience, companies must train the teams they have but be clear about the specific skills they need.

Alongside talent, respondents said that increasing data, analytics, and data interconnectivity across products and platforms is critical to improving cyber risk preparedness. Managing cyber risk is becoming a strategic priority for the second line, drawing significant investment and requiring strict prioritization. Insurers have access to large amounts of sensitive data that need protection. Even sophisticated, large carriers with significant investments in cybersecurity are not immune to such threats. In addition, the costs of cyberattacks are on the rise because of increasing fines, business losses, and remediation costs, and they often have significant reputational impact as well.

The key to success for carriers in the second line of defense is to conduct targeted reviews based on cyber risk scenarios and triggers for risk threats. 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.

Another major challenge area for risk remains climate. 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.

Our survey found that climate risk ownership is split among participants, with some assigning it to the CRO and others to the chief sustainability officer. Most participants see gaps in all areas of their climate risk framework. The reporting framework seems to be the most advanced area of preparedness, followed by exposure strategy and investment in data and analytics to baseline portfolio emissions (Exhibit 2).

Interestingly, however, most participants seemed unphased by the climate stress test methodology of the European Insurance and Occupational Pensions Authority (EIOPA). Some stated that it has limited applicability to them, while others said they are already fully in line with its recommendations.

Looking at the broader topic of sustainability, our survey found that the board, shareholders, employees, and regulators were the key influences of company efforts—despite the widespread perception that retail clients' opinions are driving actions to mitigate reputational risks.

Transforming the risk function

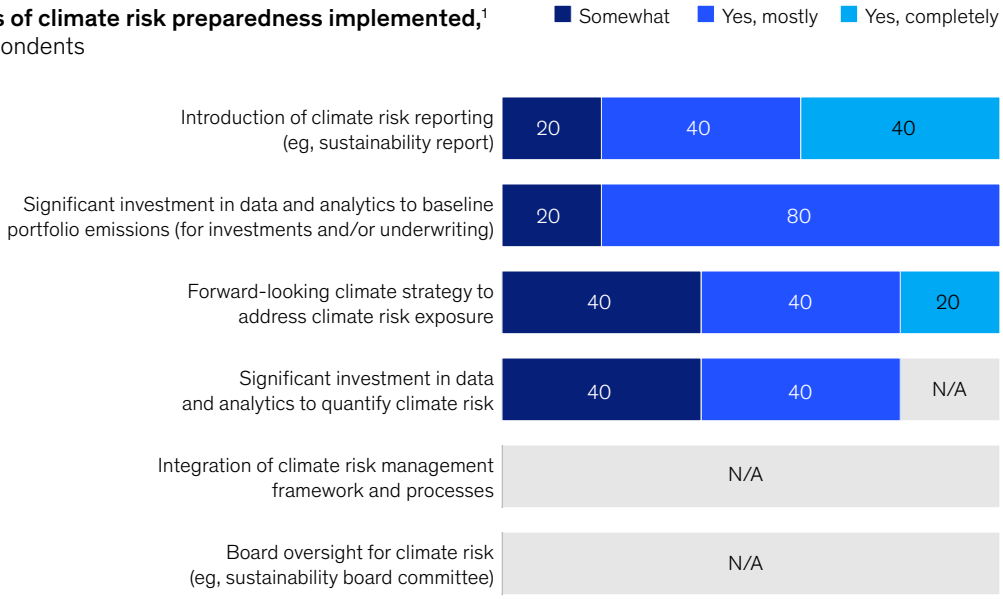
Across all insurers in our survey, it is clear that the role and status of the CRO, as well as the risk function itself, must evolve to address emerging challenges. Among our survey's respondents, the size of the risk function varies broadly from 0.07 percent to 2.8 percent of the total workforce (0.8 percent on average), while the average risk budget represents only 0.3 percent of operational expenses. These findings imply varied operating models with no market best practice.

As for the actual role of the CRO, along with risk-based decisioning, managing the relationship with the CEO and board of directors, communicating the company's risk position, and aligning the

Exhibit 2

Climate risk, led by the chief risk officer or chief sustainability officer, currently appears to focus on reporting and baselining.

Elements of climate risk preparedness implemented,[1]
% of respondents



[1]Question: Please indicate which of the following your organization has enacted or put in place relating to climate risk preparedness?
Source: McKinsey European Insurance Risk Survey, 2023

McKinsey & Company

organization's overall risk appetite and framework are becoming core activities. Only 34 percent of survey participants said that the second line has veto power on important decisions today, and just 17 percent said business units' decisions are often changed as a result of a collaboration with or challenge from the risk team (Exhibit 3).

Inconsistent adoption of best practices

In our work with organizations, we have identified four best practices for involving risk in decision making, and none of these have been fully adopted by insurance companies in our survey. At best, these practices are often only partially implemented.

— *Explicit processes for risk dialogue.* Two-thirds of our respondents have fully implemented processes to ensure that a comprehensive risk dialogue occurs, even in instances when time or confidentiality constraints prevent the use of normal corporate processes (for example, sudden opportunistic investments).

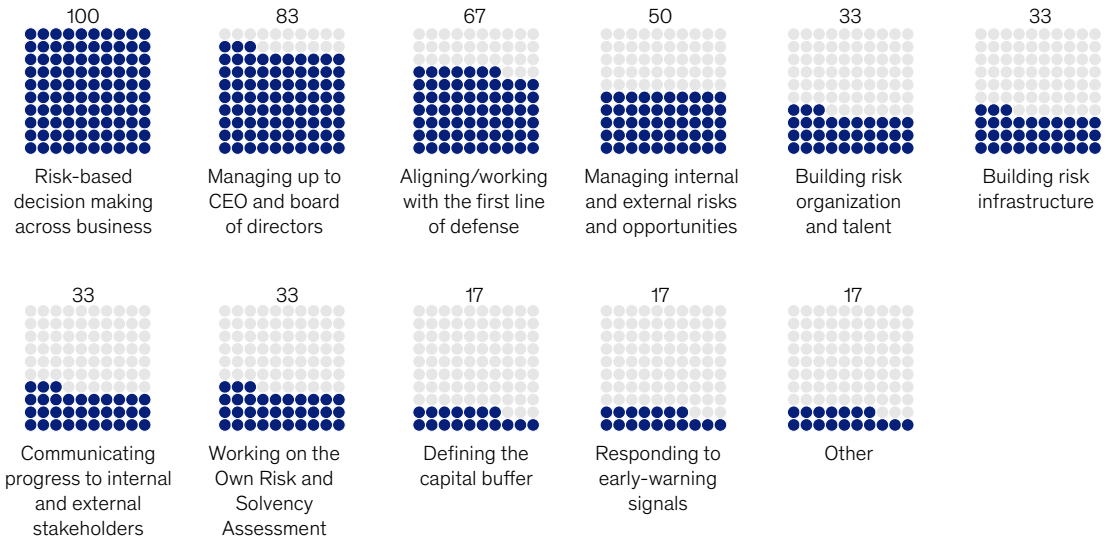
— *Transparent criteria for decisions.* Two-thirds of our respondents have fully implemented a transparent set of criteria that the risk function applies to key event-driven decisions (for example, impact on volatility, capital, and the regulatory remediation program).

— *Involvement in strategic decision making.* Half of our respondents said the CRO is fully and consistently involved in strategic decision making, with the right to either veto or escalate a strategic decision—overruled only by the CEO. The impact on the overall risk profile, appetite, and risk strategy is consistently considered in making strategic decisions.

Exhibit 3

Managing the risk position up to the CEO and board has become a core activity for chief risk officers.

Top 5 activities for chief risk officers,[1] % of respondents



[1]Question: Across any given month or quarter, which of the following activities do you consistently spend the most time on? Please select up to 5 top activities.
Source: McKinsey European Insurance Risk Survey, 2023

McKinsey & Company

— *Active risk mitigation.* Just a third of respondents said that they are actively mitigating risks to the fullest extent prior to commitment (for example, pilots and staging). It is somewhat concerning that 17 percent report having no active risk mitigation whatsoever.

Next steps

In terms of next steps for insurers looking to improve the risk function and integrate it more completely into daily decision making, we suggest fully implementing the four best practices described above, while keeping the following goals top of mind as they continue to transform the risk function:

— elevate the risk function to the forefront of the strategic agenda; give the CRO a seat at the table, with appropriate CEO and executive committee touchpoints.

— rethink the risk function operating model in terms of lines of defense, ensuring the right governance for risk management and efficient and effective interactions with business units and other control functions

— ensure that risk has appropriate resources in terms of talent and analytics capabilities

— use the risk function as a source of competitive edge—not only as a control function—by, for example, considering results from postmortem analyses and involving risk in financial planning and strategy building

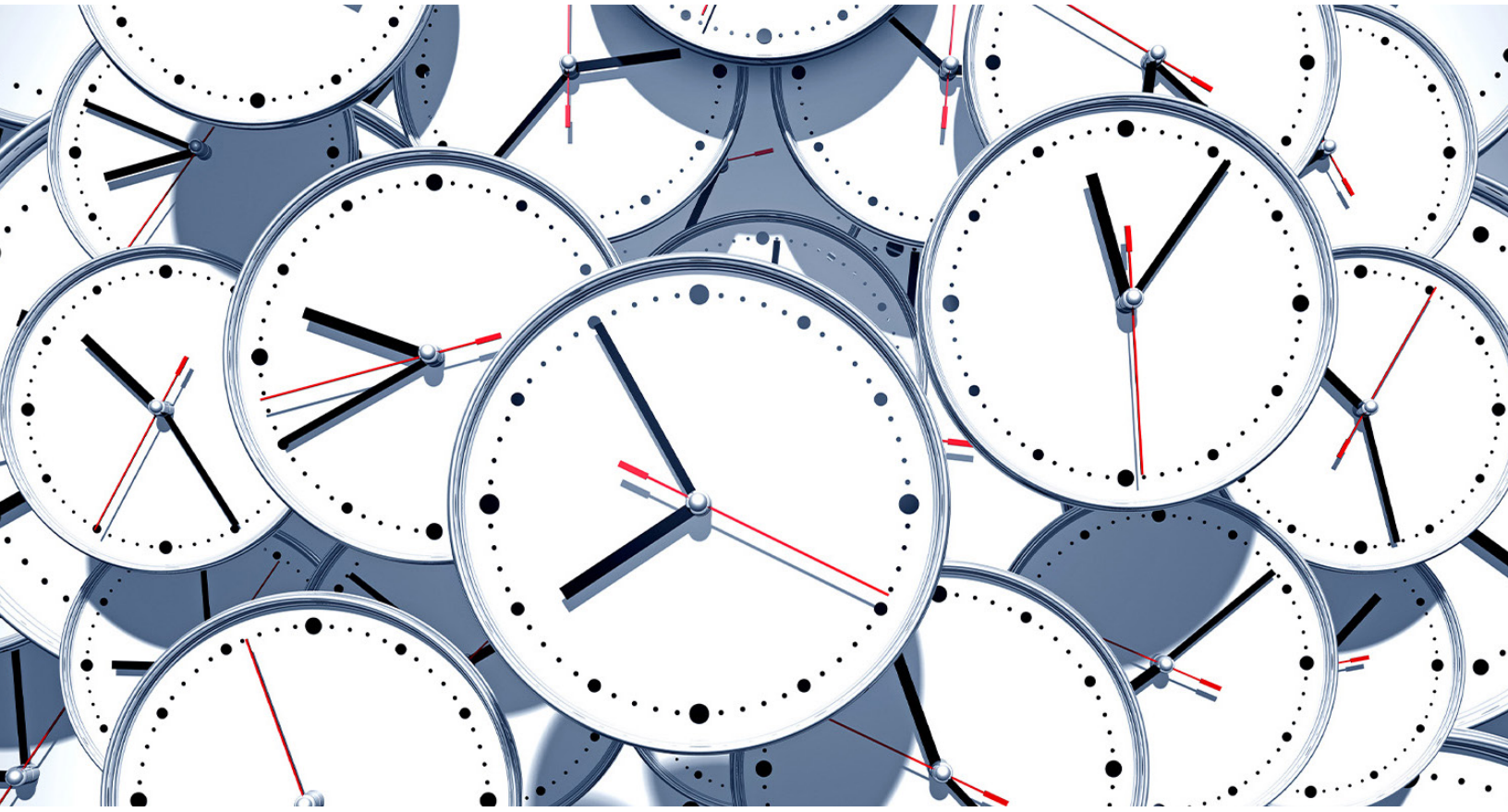
Today's rapidly developing risk landscape demands a new, more forceful, and swifter approach to assessing and responding to risk. While corporate leadership does involve the risk function in their decision-making progress, the transition from a consultative unit to a real thought partner is far from over. CROs need a seat at the table with genuine authority, resources, and support to reorganize their risk functions, build out the necessary capabilities, and influence business decisions. Elevating the risk function in this manner will allow insurers to transform risk management from its historic role as a control function to a source of strategic advantage to grow the business.

Diego Mattone is a partner in McKinsey's Zurich office, **Luca Pancaldi** is a senior partner in the Milan office, **Mina Jurisic** is a partner in the Paris office, and **Daniel Kaposztas** is a capabilities and insights expert in the Frankfurt office.

BCBS 239 2.0 resurgence: Strengthening risk management and decision making

A renewed focus on the 2013 data risk management regulatory standard poses new challenges and opportunities for European and US banks. Achieving compliance will take a structured, top-led approach.

This article is a collaborative effort by Asin Tavakoli, Holger Harreis, Kayvaun Rowshankish, and Stephen Reddin, with Cécile Prinsen, Elias Tsoukatos, and Satyajit Parekh, representing views from McKinsey's Risk & Resilience Practice.



The Basel Committee on Banking Supervision (BCBS) issued its standard number 239 (BCBS 239) nearly a dozen years ago in 2013, with the aim of strengthening banks' risk management through improved risk data aggregation and internal risk reporting. Its binding compliance deadline for global systemically important banks (G-SIBs) was nearly nine years ago, in January 2016. For domestic systemically important banks (D-SIBs), compliance was expected within three years following their designation as such.

However, full compliance remains elusive for many institutions; meanwhile, regulators are renewing their attention and applying an increasingly forceful approach. There's a broadening of scope in terms of which institutions are receiving regulatory attention—including Tier 2 and Tier 3 institutions. The assessments are also deepening in their application and level of detail across areas of policy, capability, and reporting. In Europe, they take the form of on-site inspections (OSIs), targeted reviews of priority areas, and assessments of data quality related to supervisory reporting. These actions often lead to significant penalties, including findings communicated in the form of European Central Bank (ECB) letters, Pillar 2 requirement (P2R) add-ons, restrictions on business activity, and fines. In the United States, assessments involve examinations of the data management practices of banks, along with evaluations of related areas such as regulatory reporting, resolution and recovery planning, and specific report examinations (for example, the Complex Institution Liquidity Monitoring Report, or FR 2052a). These assessments can result in matters requiring immediate attention (MRIAs) and matters requiring attention (MRAs); in the most severe situations, they may lead to consent orders. Across both Europe and the United States, beyond the direct penalties, there are cascading indirect financial consequences, such as conservatism add-ons in risk modeling, for example, margins of conservatism (MOC) for internal ratings-based (IRB) models.

A renewed call to action

According to the Bank for International Settlements, only two in 31 banks (G-SIBs) have fully complied with the standard; moreover, several formerly compliant banks have been downgraded. A series of progress reports—seven between 2013 and 2023—issued additional regulatory guidance. The sixth report, which in April 2020 called for the transition of enforcement to local regulators, was followed by a pause of approximately three years. This pause, however, concealed the growing pressure on banks to meet the expectations of local regulators. In Europe, this includes the issuance of ECB letters with findings, P2R add-ons, and fines. In the United States, banks face scrutiny from the Office of the Comptroller of the Currency and the Federal Reserve Board, including MRIAs, MRAs, and, in severe cases, consent orders.

This pressure was ratcheted up considerably by the latest report in November 2023, which highlighted a lack of meaningful progress and issued significant expectations for banks and their supervisors. The report noted that BCBS 239 programs have been underfunded and lacking in attention from senior leadership, with insufficient recognition of the standard's importance in relation to capability improvement. It also pointed out a failure to embed the standard in relevant urgent programs, such as Basel IV/3.1. Contributing to the lack of progress, the report suggested, is a "boil the ocean" approach taken by some banks, with insufficient prioritization of requirements and misfires with regard to the scope of implementation. Technical factors, including fragmented IT ecosystems hampered by legacy systems, add to the struggle.

In addition to the BCBS 239 progress reports, regulatory bodies have called attention to related problems. The ECB's banking supervision identified risk data aggregation and risk reporting (RDARR) deficiencies in its December 2023 report on supervisory priorities for 2024–26. Likewise, its May 2024 *Guide on effective risk data aggregation and risk reporting* (*Guide*) conveyed a range of guidance, including highlighting the importance of basic data governance hygiene to ensure confidence in the numbers and reports issued by financial institutions, clearly defining what constitutes critical risk and finance information across various dimensions, prioritizing end-to-end automated lineage, and actively involving top management. The *Guide* also adds, for the first time, real practical guidance on essential requirements across seven areas—leaving no room for neglect.

Guiding principles for success

We are aware of the obstacles encountered when endeavoring to manage risk-related data effectively. In line with the latest BCBS 239 progress report, we've identified a number of key challenges that need to be addressed. These include getting organizations with differing priorities and perspectives to work together, conducting thorough root-cause analysis to identify data issues in a context where data are pervasive throughout the bank, and aligning existing incentive structures to promote a strong data management culture. We have five core beliefs, along with ten key lessons (see sidebar, "A blueprint for success"), about how banking organizations should orient their mindset when it comes to BCBS 239. By finding the right disposition toward the standard, financial institutions can position themselves well to undertake meaningful action. Consider these five guiding principles the foundation for an effective strategy blueprint—and as part of that blueprint, aim to create visibility for board and senior management with frequent progress reports.

1. Make it a business impact story from the start

It's crucial—and truly beneficial—to approach the BCBS 239 journey as a business impact story right from the beginning. This means the CFO, chief information officer (CIO), and chief risk officer (CRO) should be proactive in bringing the business leaders on board and linking the effort to specific business objectives that go beyond regulatory compliance. Leaders should highlight the opportunities that arise from more timely data and streamlined calculation processes in prioritized areas. Improved master and transactional data can unlock new commercialization opportunities. Additionally, improved model explainability can mitigate the impact of regulatory reviews. Leaders should develop a perspective focused on how initiatives can be linked and integrated with existing business-related efforts and programs.

Our experience suggests that practical implementation of such an approach entails interviewing business leaders at the outset to identify major data-related pain points and prioritize the respective remediation. This could include initiatives such as shedding excessive hedges and capital buffers currently in place due to insufficient timeliness of risk metrics or removing margins of conservatism while remaining within the boundaries established by risk modeling.

2. Take a risk reduction approach from the outset

Leaders should identify and prioritize critical information, addressing these areas first to immediately mitigate the most significant risks. With the scope prioritized at the beginning, it can then be expanded in terms of both breadth and depth. For example, banks might begin with an initial prioritized scope in the form of select key regulatory reports and management metrics, focusing on data quality controls and the reduction of manual interventions in high-risk areas of the aggregation processes. Then, in time, the prioritized scope can expand to include a broader set of reports and metrics, with data quality controls across more points in the aggregation processes. In essence, this approach entails breaking the scope into manageable sizes while enabling the measurement of risk reduction in critical outputs.

Our experience suggests that the above can be achieved by ensuring risk and finance collaboration from the beginning of the program and tasking the respective areas with identifying the information most critical to them. This can then be conveyed in terms of common dimensions such as metrics, critical data elements (CDEs), and reports based on central guidance regarding what constitutes criticality. There should also be a focus on sharing/reusing CDEs across the metrics so that the population does not keep growing unnecessarily.

3. Look for opportunities to accelerate execution

Leaders should look for opportunities to accelerate the execution of the approach described in principle 2. The use of generative AI (gen AI) tools can significantly accelerate data compliance and development efforts. In fact, leading organizations are deploying gen AI at scale to fix data quality issues and go beyond rule-based vendor products, enabling significant value through higher productivity.

A blueprint for success

With the five guiding principles we mentioned earlier serving as the foundation, we can present ten key lessons learned for a successful BCBS 239 approach.

Lesson 1: Ensure the business is also made accountable. Create messaging—right from the top—that the business is also accountable; moreover, leaders should strengthen the chief information officer's (CIO) role in funding decisions to ensure alignment with data program objectives.

Lesson 2: Set realistic targets and deliver via incremental spend add-ons. Be conscious of the difference between "must-haves" and "nice-to-haves" in terms of meeting requirements, and articulate clear priorities to meet minimum requirements first. Insofar as it is possible, add the prioritized requirements to the existing risk data portfolio of interventions and adequately increase the budget.

Lesson 3: Balance short-term and longer-term initiatives. Put in place a program that will enable the CFO, CIO, and/or chief risk officer (CRO) to demonstrate short-term progress (for example, addressing backlog data issues and critical data issues affecting regulatory capital models) while beginning longer-term efforts, such as adopting new end-to-end lineage tooling solutions.

Lesson 4: Ensure the board takes full responsibility. Make sure that incentive schemes (for example, bonuses and remuneration) are linked to the achievement of the goals and that members have or build up sufficient knowledge and experience in risk data aggregation and risk reporting topics (that is, data management, IT, risks).

Lesson 5: Create visibility and trust with regulators. Visibility is essential not only for senior management but also crucial for the relationship between banks and regulators. Establish trust by communicating about prioritization and approach to implementing capabilities; meanwhile, build a structured method for regular progress reporting.

Lesson 6: Engage and empower key talent. Position the right people with the right skills, knowledge, and experience to orchestrate processes effectively. For example, a CRO who is close to the key risk data-related regulatory priorities and programs and a chief data officer with detailed knowledge of the business data are well positioned to help drive success.

Lesson 7: Balance regulatory and business data requirements. Maintain an understanding that while urgent regulatory requirements must be addressed, data must also support concurrent business objectives such as revenue growth, customer satisfaction, and operational efficiency.

Lesson 8: Embrace a clear data domain framework. Use a data domain framework as the organizing construct for data, including elements such as authorized sources, controls, and accountable owners. Moreover, establish strict rules for domain management (for example, reconciliation to ledger) and thoughtful processes to prioritize the rollout of the domains.

Lesson 9: Enforce design principles. To succeed in changing the way of operating, adhere to design principles. Such principles might prohibit unilateral decisions, for example, or establish that the front office must use the same data sets as other functions.

Lesson 10: Spend time to structure and prioritize. Develop the overall blueprint for risk and finance data requirements and deliver these in prioritized and efficiently grouped waves.

We have observed that, as a starting point, banks can benefit from tools that help automate data lineage and transparency efforts to ensure base levels of compliance. This approach will also provide banks with a clear view of the gaps and issues in their data. With this in place, banks can take directed actions to remediate data issues. Next, banks should think through the entire data development life cycle to understand what types of tools and interventions are needed. Gen AI tools, for example, can help integrate data privacy and protection solutions during the data governance stage. Banks should consider experimenting with a suite of tools to build deployable data quality workflows—focusing not only on which ones can best support their development needs but also on those that can do so at scale.

4. Remediate at the source with a target architecture and operating model to guide the process

Banks should aim to remediate data as far upstream in the data life cycle as possible, ideally at the point of origination. Ideally, they should move toward a target data architecture that relies on a limited number of authorized provisioning points (APPs) or authoritative data sources (ADSs). Implementing a robust set of data controls, preferably automated and preventative, early in the data process is crucial to ensure quality for downstream consumers. It is important to rigorously enforce the use of APPs and ADSs to ensure that high-quality data are sourced from a minimal set of systems. If existing data sources fail to meet consumer requirements, they should be upgraded, rather than creating new, redundant sources, which would require additional controls and governance to maintain data quality.

Experience tells us that most data quality issues originate from upstream systems in the data sources and at the consumption point. To address this, banks can, as part of their data operating model, map the data lineage from its point of origin to its consumption point. This enables evaluation of the existing data controls to determine their effectiveness and gather feedback on pain points from data consumers throughout the lineage—thus identifying where additional data controls and/or upgrades are necessary. Banks should consider implementing a comprehensive framework that outlines minimum preventative, detective, and corrective data quality control requirements for critical data along the end-to-end data lineage.

5. Be transparent and comprehensive in regulatory dialogue

Banks should maintain a strong degree of proactiveness and transparency with regulators, ensuring they perceive the bank and the BCBS 239 program as models of openness and proactivity. To convey a strong sense of control and oversight, it is important to communicate in a highly structured manner, providing regular progress reports that offer comprehensive information on both the current status and upcoming initiatives. Insofar as possible, banks should implement initiatives of their own accord versus waiting for a regulatory push. This approach will enable the bank to set its own pace.

In our experience, this entails communicating early on the scope of the program—as well as the vision, ambition level, and execution approach (for example, deciding to first do a horizontal fix of all foundational aspects versus engaging a sprint-based method). Thereafter, this involves building and leveraging structured templates to communicate the current state (for example, gaps in critical metrics) and upcoming initiatives; likewise, it includes regular reporting on progress and bottlenecks. Where possible, banks should inform the regulator in an integrated way, such as by communicating BCBS 239-related initiatives and commitments as part of Basel IV/3.1 programs.

It is important to communicate in a highly structured manner, providing regular progress reports.

Banks across Europe and the United States are at varied stages of maturity

European and US banks vary widely in terms of where they stand on their BCBS 239 journeys. Some are just beginning, while others are refreshing their efforts or accelerating their progress. Those furthest along have been dedicated to compliance for several years. They have been closely monitoring key risk metrics and reports, with business and IT functions closely involved. Nevertheless, they face regulatory scrutiny, because BCBS 239 demands perpetual enhancements, such as the removal of manual processes and the widening of scope across dimensions of reports, models, risk indicators, and critical data elements, with the ultimate aim of covering all critical data of the bank.

Banks in the middle of their BCBS 239 compliance journey typically have well-documented frameworks, such as data governance structures, clearly defined scopes, and have begun exploring new tools. However, they often struggle to make swift, measurable progress and engage the business. Some of those just starting out have previous failed attempts behind them. The problem typically lies with execution: despite ambitious plans, practical implementation has proved elusive, and tooling sometimes emerges as an excuse.

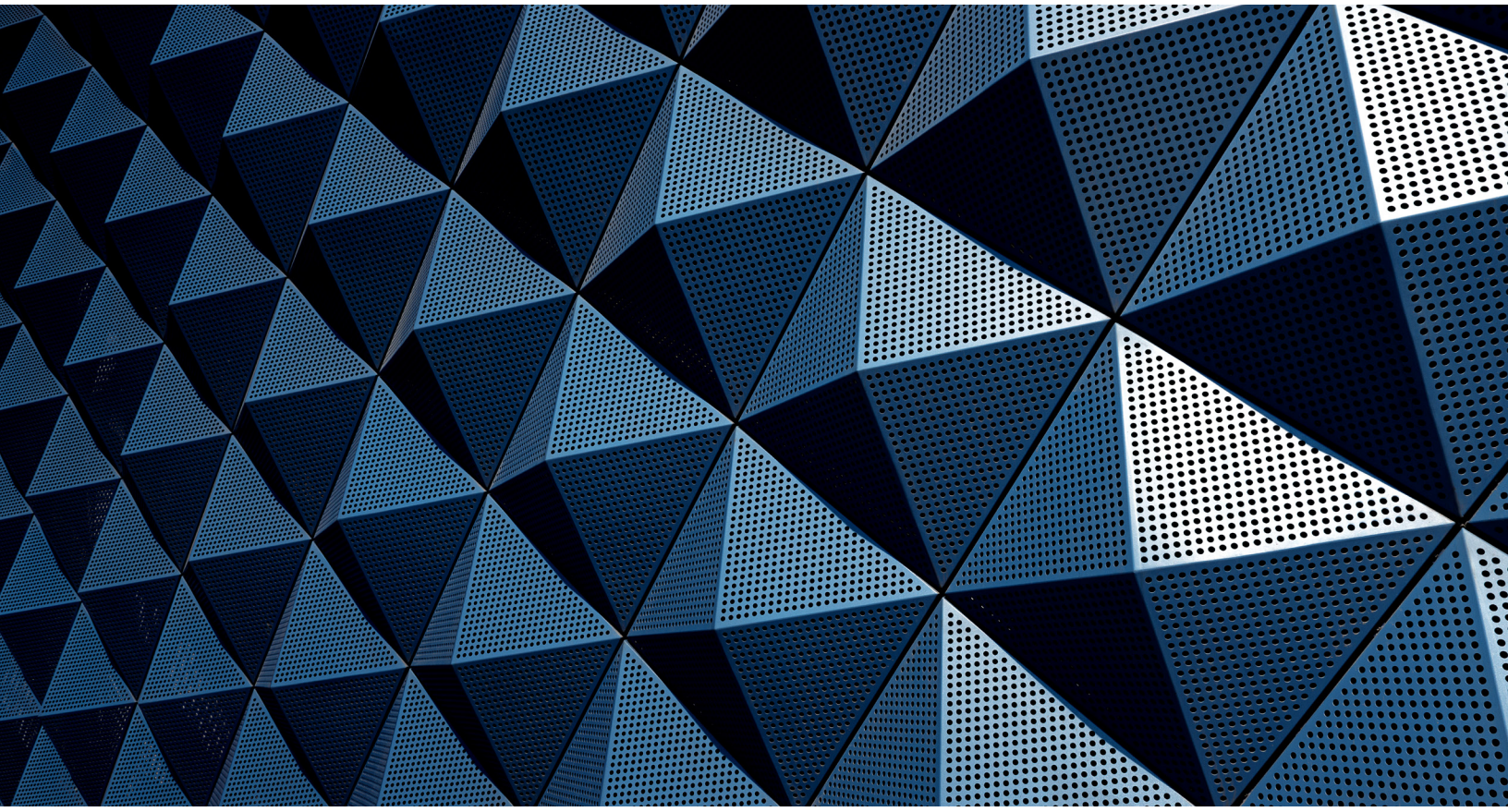
The rewards are worth the effort. Banks are at an important moment in their regulatory journeys. With BCBS 239 getting renewed attention and the expectations rising rapidly, the pressure is on to make meaningful progress toward full compliance. By establishing a business impact mindset across the organization, these requirements can also become an opportunity for competitive advantage with a host of indirect financial benefits, including enhanced digitization initiatives, improved risk management, and bolstered relationships with regulators based on trust.

Asin Tavakoli is a partner in McKinsey's Dusseldorf office, where **Holger Harreis** is a senior partner; **Cécile Prinsen** is an associate partner in the London office; **Elias Tsoukatos** is an associate partner in the Athens office; **Kayvaun Rowshankish** is a senior partner in the New York office; **Satyajit Parekh** is an associate partner in the Boston office; and **Stephen Reddin** is a partner in the Toronto office.

The European Union AI Act: Time to start preparing

A successful digital future depends on responsible use of AI. The EU AI Act marks a significant step in regulating AI systems and could serve as a blueprint for other jurisdictions.

This article is a collaborative effort by Henning Soller with Anselm Ohme, Chris Schmitz, Malin Strandell-Jansson, Timothy Chapman, and Zoe Zwiebelmann, representing views from McKinsey's Risk & Resilience and Digital Practices.



Artificial intelligence and generative AI (gen AI) will have a transformative impact on economic growth and productivity. This is especially true for organizations that expect to make changes to their operations using the technology, a recent McKinsey survey shows.[1]

To realize the benefits of AI, organizations need the underlying models and their use to be secure, safe, and trusted. Implementing robust data governance, model-risk, security, and individual-rights management is crucial for responsible AI governance. Together, these pillars create a solid foundation for future digital transformation, and digital trust. According to McKinsey research, trusted organizations have higher margins and better valuations than less-trusted ones.[2] And while only a small contingent of companies are set to deliver this digital trust, organizations that are best positioned to build digital trust are also more likely than others to see annual growth rates of at least 10 percent on their top and bottom lines.

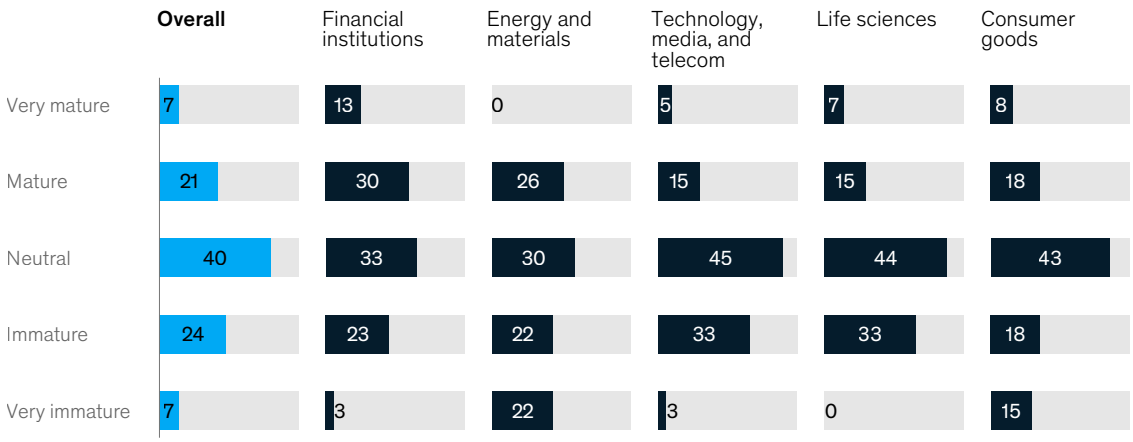
While many organizations embrace these concepts, some still lack fundamental risk controls for the new technologies. In early 2024, McKinsey surveyed 180 EU-based organizations in five sectors about the state of AI governance in the European Union. Seventy-one percent of respondents said their AI risk governance was less than mature, although 65 percent of them said they were already using gen AI (Exhibit 1).

Survey participants expressed concerns in five high-level categories that mirror important considerations for AI: data, model output, security, third-party, and societal risks.

Exhibit 1

Less than 30 percent of survey respondents consider their organization's AI risk governance to have some level of maturity.

Maturity of organization's AI risk governance,[1] % of respondents



Note: Figures may not sum to 100%, because of rounding.
Question: How mature is your AI risk governance?
Source: McKinsey EU AI Act Survey, spring 2024 (n = 180 organizations in Europe)

McKinsey & Company

[1] "The state of AI in early 2024: Gen AI adoption spikes and starts to generate value," McKinsey, May 30, 2024.
[2] Jim Boehm, Liz Grennan, Alex Singla, and Kate Smaje, "Why digital trust truly matters," McKinsey, September 12, 2022.

Some concerns fall into one category, while others span several. Bias, for example, touches model output, data, and third-party risk. Among the other potential concerns expressed in the survey are discrimination, bad outputs, personal-data leakage, intellectual property misuse, security breaches, and malicious use.

Given everything that could go wrong with AI, standards and policy setters are increasing efforts to control the risks. Regulators globally are introducing regulatory frameworks and guidelines, including in Canada, China, Japan, South Korea, and the United States. The EU AI Act, enacted by the European Union in May 2024, is the world's first general AI regulation to go into effect. Being the first of its kind, the EU AI Act will serve as a test bed for other guidance to follow. In addition, it will have extraterritorial effects because the scope includes AI tools developed in other markets if a tool or its output is applied in the European Union.

Overview of the EU AI Act and its requirements

The EU AI Act aims to "promote human-centric and trustworthy AI while protecting health, safety, and fundamental rights." It will have wide-ranging implications for all affected organizations as the guidance is rolled out over the next two years.

The act sets requirements in four areas: governance, data management, model-risk management, and individual rights. These requirements include risk and quality management, human oversight, AI system documentation and transparency, data management, model-risk governance measures for nondiscrimination and bias, accuracy, robustness, and cybersecurity.

Which requirements apply to each organization depends on two factors: the risk classification and the role of the organization in the AI value chain, which includes providers, importers, distributors, deployers of AI systems, and combinations thereof.

Based on the use case, AI systems are defined as prohibited, high-risk, or non-high-risk. Rules for "prohibited" AI, which includes models that are manipulative or deceptive, are outlined in Article 5 of the act. "High risk" systems are those that could threaten health, safety, and fundamental rights, including those related to critical infrastructure, education or vocational training, employment, access to essential public or private services and benefits (including credit and health insurance), profiling, and law enforcement. "Non high risk" systems, with lower or no regulatory requirements, consist of everything not specifically covered by the other two categories, including AI in video games and customer service chatbots.

Early days of implementation efforts

AI governance and EU AI Act compliance efforts are still in the early days, but organizations already have questions. More than 50 percent of survey respondents said they are not clear on AI act requirements and are unsure of the risk classifications for their AI use cases (Exhibit 2).

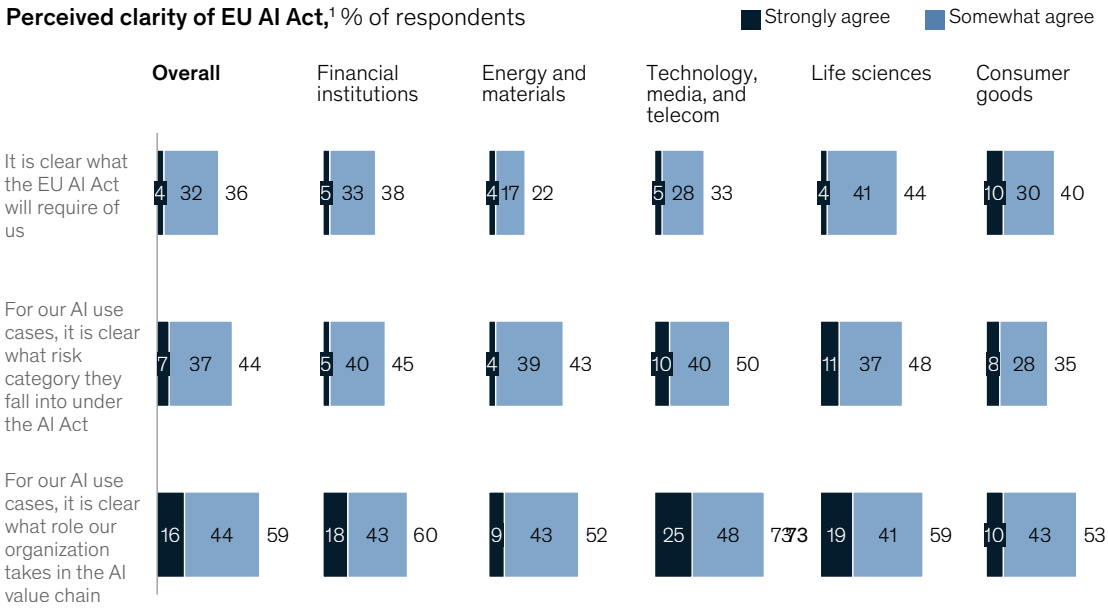
Organizations consider themselves most prepared with regard to data management, ahead of governance, model risk management, and individual rights (Exhibit 3).

Even so, data management is still a concern. More than half—57 percent—of respondents said that many data governance requirements remain unaddressed. Specifically, some organizations said there is a lack of clarity in terms of how the General Data Protection Regulation (GDPR) and the EU AI Act will interact.

When asked whether they had already met the act's requirements for the four areas, less than 10 percent of survey respondents said that they had (Exhibit 4).

Exhibit 2

Only 4 percent of survey respondents agreed that the EU AI Act requirements are clear.

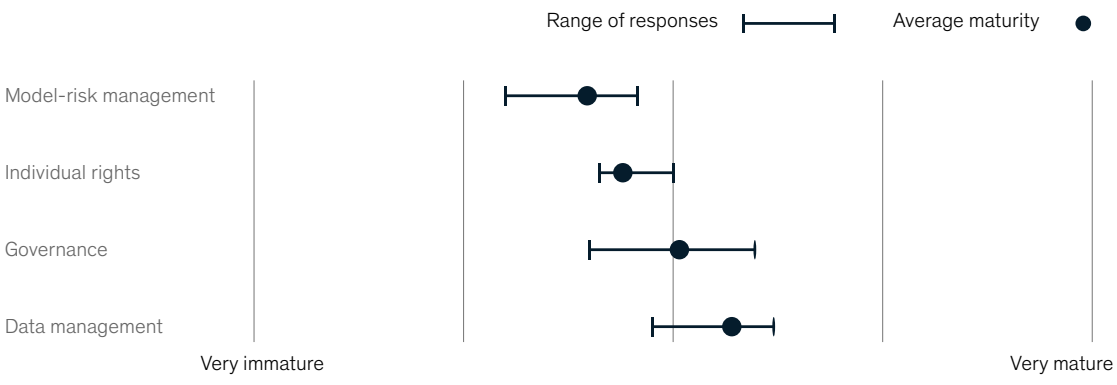


Note: Figures may not sum to totals, because of rounding.
Question: To what extent do you agree with the following statements?
Source: McKinsey EU AI Act Survey, spring 2024 (n = 180 organizations in Europe)

McKinsey & Company

Exhibit 3

Survey respondents consider their organizations somewhat prepared across various dimensions of the EU AI Act.

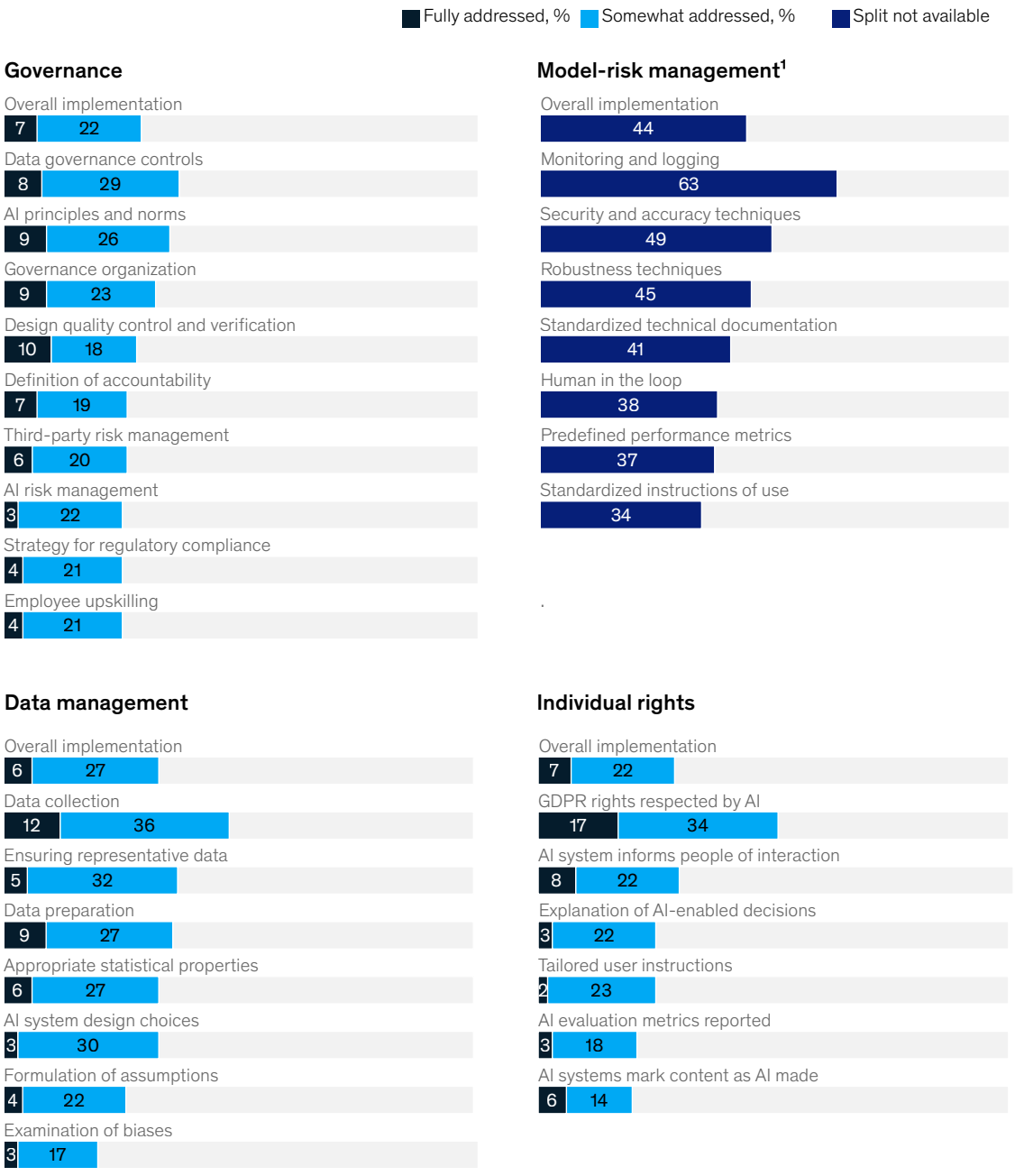


Source: McKinsey EU AI Act Survey, spring 2024 (n = 180 organizations in Europe)

McKinsey & Company

Exhibit 4

Few of the key requirements of the EU AI Act are fully addressed by more than about 10 percent of organizations.



[1]Based on proportion of organizations having technically implemented these measures, not the level at which they have addressed them.
Source: McKinsey EU AI Act Survey, spring 2024 (n = 180 organizations in Europe)

McKinsey & Company

Nearly half of respondents said they had not yet allocated any budget for AI Act implementation, and most that have allocated a budget have set aside €2 million or less (Exhibit 5). There are many reasons organizations aren't spending yet. Some respondents have likely not started responding to AI Act requirements because the rules are so new. Others are focused on aligning their AI remediation efforts to their existing governance structure. Still others are unaware of the upcoming regulatory requirements.

Key challenges facing organizations

Respondents cited a variety of challenges to their efforts to meet the requirements of the AI Act.

Complexity. In some cases, organizations are stalled as they seek clarity and the resources to prepare for complex regulations and technology. Only one in four survey respondents have implemented strategies for regulatory compliance or AI risk management.

Risk governance. About three in ten respondents have developed a mature AI risk governance structure, and only a third said they have a governance organization. Further, about 40 percent lack clear definitions of accountabilities for AI, and about 10 percent say they have fully addressed AI principles and norms.

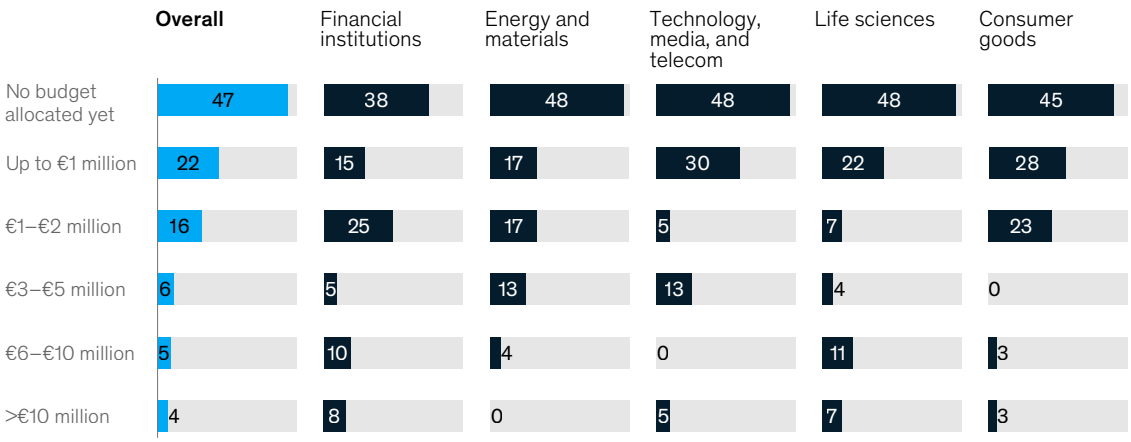
Encouragingly, nearly half of respondents said they have separate usage guidelines, and more than a third have input and output guardrails in place for external AI models. This likely is a consequence of protecting business-sensitive information and intellectual property as organizations rapidly deployed gen AI tools.

Third-party risk management is also a concern. Less than a third of organizations said they have appropriately addressed AI-related third-party risk.

Exhibit 5

Close to 50 percent of organizations have not yet allocated resources for EU AI Act implementation efforts.

Amount budgeted for EU AI Act implementation efforts,[1] % of respondents



Note: Figures may not sum to 100%, because of rounding.
Question: How much have you budgeted for EU AI Act implementation efforts?
Source: McKinsey EU AI Act Survey, spring 2024 (n = 180 organizations in Europe)

McKinsey & Company

Some have implemented GDPR-related controls, technical guardrails, and model fine-tuning for external models. But just 16 percent of respondents are conducting red-teaming efforts, while some said they are rolling back relationships with suppliers while rules and obligations for general-purpose AI become applicable throughout 2025.

Data governance. Only 18 percent of respondents said their organizations have mature technical risk management processes for AI systems in place. In addition, few have robust models or security and accuracy techniques. However, about 75 percent of respondents indicated they had advanced cyber controls and data protection measures in place.

The act introduces requirements for data management. These cover choices in designing systems, formulating assumptions, collecting and preparing data, examining bias, ensuring representative data use, and including the appropriate statistical properties. More than half of survey respondents said they have not yet addressed these requirements. Less than 20 percent have addressed bias.

What models do with the data is another area of concern. Many respondents cited difficulty in defining standards for testing the outputs of gen AI models. For self-developed models, respondents said they commonly use continuous code integration and deployment, model versioning, and documentation to ensure quality.

Thirty-eight percent of respondents use "human in the loop" processes, while 30 percent use technically responsible AI tooling. Model performance monitoring, logging, and user feedback, together with incident detection and management, are the most common measures used to ensure quality after deployment.

Talent. Getting the right people to run and manage AI is proving difficult, too. The talent shortage is especially prominent for technical staff but also exists for legal personnel. This is a major concern not only for businesses but also for regulatory authorities that have concerns about competent monitoring and enforcement of the AI Act. Only a quarter of respondents upskill employees, which takes time and investment.

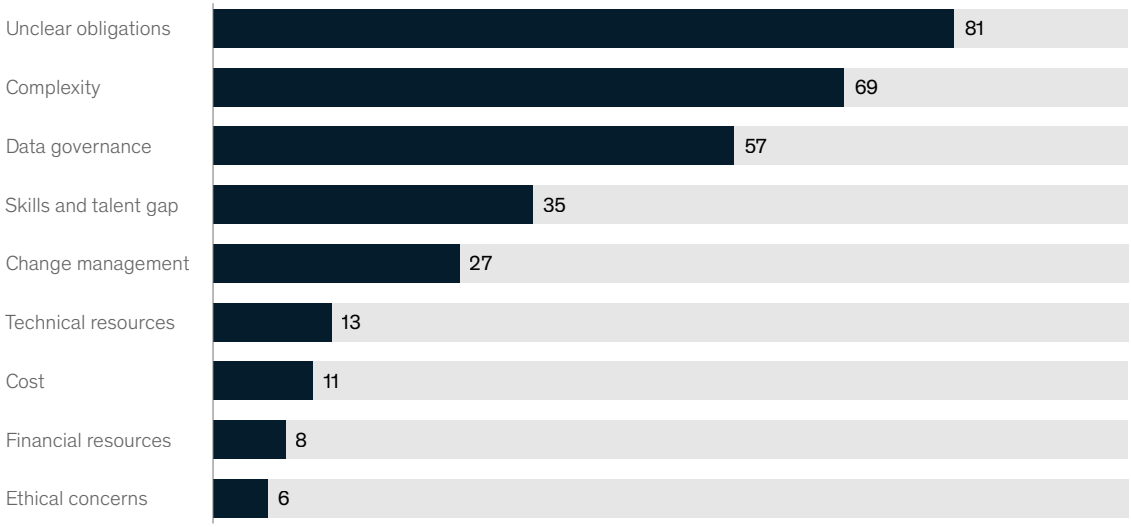
Other. Perhaps surprisingly, respondents did not cite cost, financial resources, or ethical concerns as top reasons for the slow progress on implementation (Exhibit 6).

Given the complexity of the EU AI Act and the effort needed to comply, it would be prudent for organizations to accelerate their planning now.

Exhibit 6

Key challenges of implementing the EU AI Act relate to unclear obligations, complexity, and talent gaps.

Key challenges facing organizations in implementing the EU AI Act,[1] % of respondents



Source: McKinsey EU AI Act Survey, spring 2024 (n = 180 organizations in Europe)

McKinsey & Company

The time to act

Given the complexity of the EU AI Act and the effort needed to comply, it would be prudent for organizations to accelerate their planning now. While the act outlines implementation stages and staggered compliance deadlines, those with experience implementing GDPR understand that waiting can create chaos as those deadlines approach.

Managing the scope of an organization's AI efforts is important. Organizations that align development to governance practices manage to limit the number of models they use, generally to fewer than 20. A clear governance structure can also limit teams' frustrations in fielding ad hoc requests and trying to get support.

Organizations should embrace a "define your world" approach, which prioritizes transparency in model use, stakeholders, risks, and regulations. The EU AI Act has set out requirements mainly for high-risk models, so a risk categorization of the model landscape will help structure the work going forward and control the level of effort.

Defining a target state for governance and compliance efforts can help organizations build road maps that thoroughly consider strategy, risk appetite, organizational structure, technology, policy, and tooling. And organizations can continue to get better through a process of ongoing improvement, using existing best practices and frameworks as a guide. Ensuring cross-functional collaboration and input on ethical and risk considerations is paramount, so if current risk

functions are not equipped, separate action on top of existing governance may be required.

To achieve compliance, organizations will need the necessary talent, resources, and relevant KPIs to measure progress. AI is evolving quickly, so it is essential to stay on top of changes. The EU AI Act represents a significant step toward regulating AI systems and ensuring responsible AI governance and could serve as a blueprint for other jurisdictions globally.

But before that happens, the act's regulators will need to further clarify their expectations and work with the industry to find pragmatic implementation solutions in an environment of limited resources. Responsible and trustworthy AI is a prerequisite to defining a new digital future. By embracing responsible AI governance, companies can spur innovation with the trust of consumers, competitors, shareholders, and society behind them.

This article originally appeared in the August/September edition of The RMA Journal.

Henning Soller is a partner in McKinsey's Frankfurt office; **Anselm Ohme** is a consultant in the Berlin office, where **Chris Schmitz** is a data science fellow; **Malin Strandell-Jansson** is an alumna of the Stockholm office; **Timothy Chapman** is an analyst in the Wroclaw office; and **Zoe Zwiebelmann** is a consultant in the Hamburg office.

The authors wish to thank Andreas Kremer, Angela Luget, Angie Selzer, Artem Avdeed, and Silvia Tilea for their contributions to this article.

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

Leader, Risk Knowledge
Lorenzo Serino
Lorenzo_Serino@McKinsey.com

In this issue

December 2024
Designed by LEFF

McKinsey.com