KPMG

Future of risk

Building a trusted risk function to succeed in a riskier world.

KPMG LLP | visit.kpmg.us/FutureOfRisk

Foreword

As businesses face a rising tide of risk, organizations should restructure the fundamentals of how they handle uncertainty.

Today, managing risk is riskier than ever. Enterprises are facing an array of reputational, environmental, regulatory and societal forces. And unfortunately, using the same recipe — and merely increasing the scale of your risk operation — is no longer viable. The way forward requires the C-suite to change its mindset to completely embrace risk as an enabler and an asset that can drive stakeholder value. Without that collective focus, the opportunities from the modern risk environment cannot be properly captured.

To meet these challenges, organizations should fundamentally transform their overall approach to risk. This involves giving the business clarity into the structure, function, purpose and value of risk, and aligning enterprise risk management with the strategic objectives of the business. It also requires building proactive enterprise risk capabilities, shifting the risk function from "compliance and control" to value creation, and leveraging technology, including artificial intelligence (AI) and generative AI (GenAI), to accelerate these changes.

To explore how executives expect their organizations to mitigate external and internal risks in the face of a rapidly changing business environment, KPMG International conducted a global survey of 400 executives in February and March 2024. The responses — and the accompanying insights in this paper — can inform organizations' quest to chart the future of their risk function.

The way forward requires the C-suite to change its mindset to completely embrace risk as an enabler and an asset that can drive stakeholder value.

Key insights

61% of executives expect to see a **significant increase in the level of risk** they will be responsible for in the next three to five years.

#1 For C-Suite executives, the number one factor driving a successful risk transformation is **leadership that fosters a risk-aware culture and prioritizes risk management throughout the organization.**

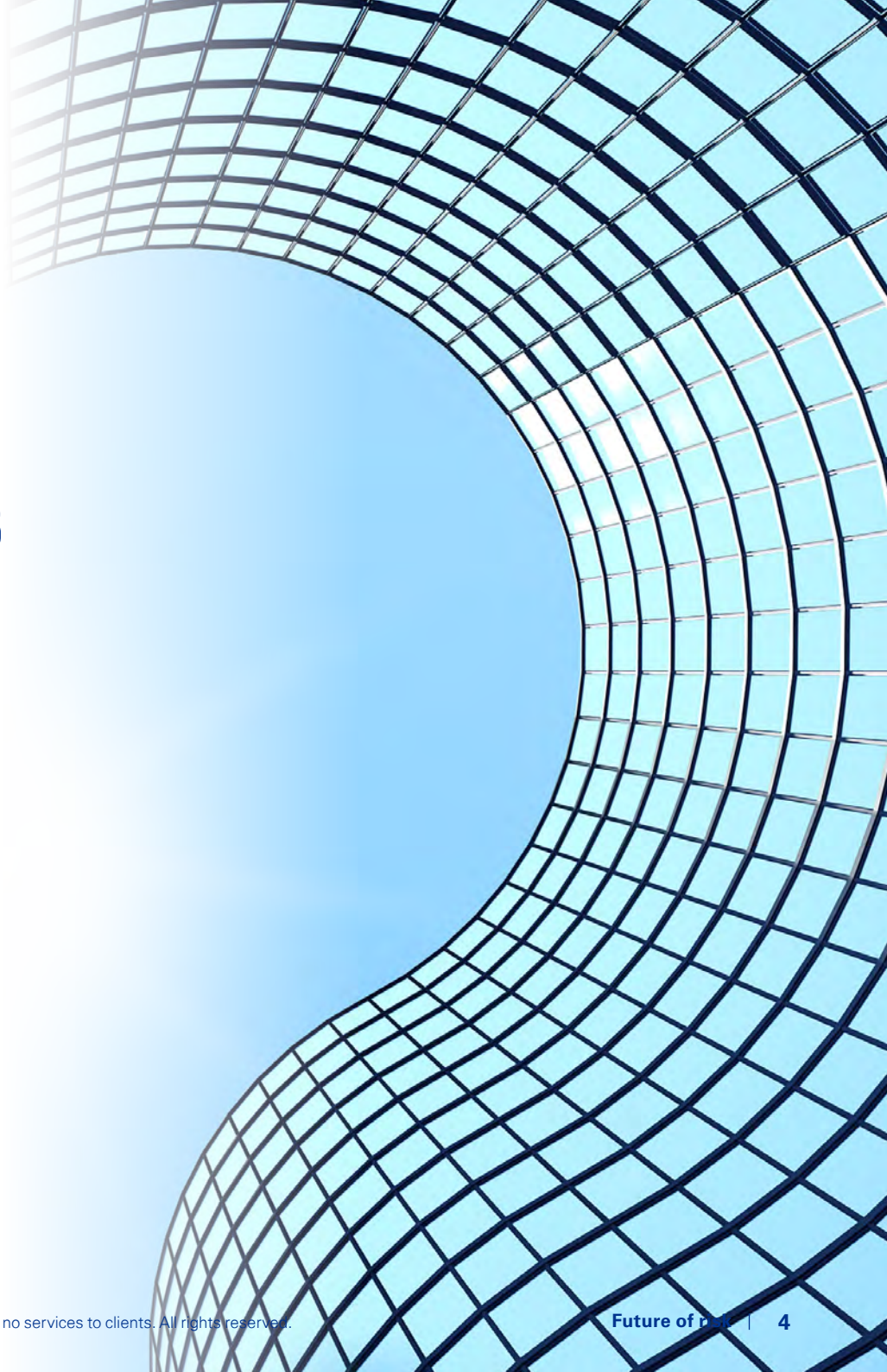
67% of chief risk officers (CROs) and risk professionals say **risk data brings an increased awareness and understanding** of potential risks and their impact on the organization.

71% of CROs and risk managers say the **integration of systems, domains and processes** can significantly enhance the effectiveness of risk-related decision-making.

41% of executives expect to spend **more than half of their risk management budget on technology** in the next 12 months compared with just 28% in the previous year.

#1 **AI and GenAI** are by far the most popular type of technologies for **managing additional risk responsibilities** in the next three to five years.

Contents



Managing risk is riskier than ever

A significant number of both internal and external factors are crashing together to make risk management more complex and challenging. From the outside, geopolitical tensions are sending shocks through every sector, impacting supply chains, financial systems, access to capital, prices of goods and commodities, and, ultimately, economic stability. In addition, incredible technological advances are combining with massive new regulatory burdens, climate change and an incredibly delicate reputational risk environment to create enterprise-wide uncertainties.

The forces pressuring businesses from the inside are equally disruptive. Even while the scope of risk continues to expand rapidly, the pressure to reduce the cost devoted to the risk function is getting ever tighter. In addition, internal issues arising from years of "tech debt" are making existing talent issues even worse, all while intensifying the competition for transformational priorities and resources. (Exhibit 1) Tech debt risk is related not only to legacy systems and processes that are not integrated and hinder the adoption of new technologies and capabilities, but is also connected to the critical mass of technological shortcuts that businesses have implemented over the years to keep up with this rapid pace of change.

Exhibit 1: Factors driving the need to reformulate risk

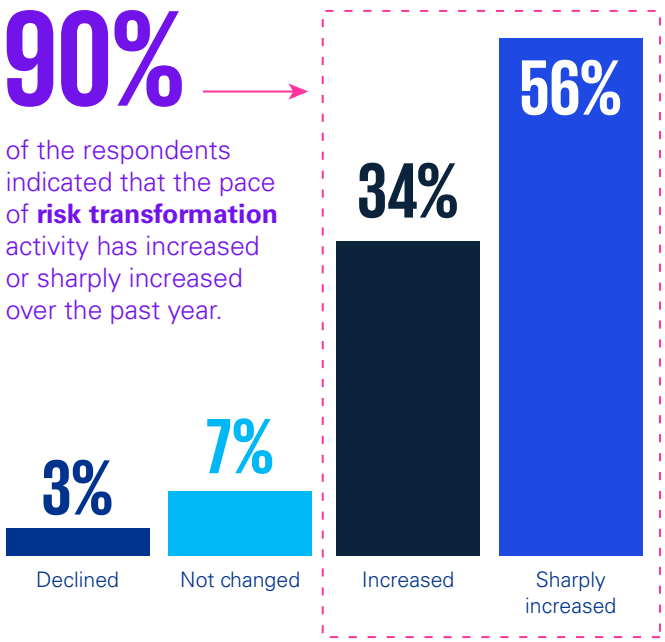
External risks	Geopolitical
	Technological
	Macroeconomic
	Regulatory
	Climate change
	Reputational
Internal risks	Increased cost pressures
	"Tech debt"
	Talent limitations
	Competing transformation priorities

The impact of these mounting pressures boldly came to life in our survey. Our findings show that risk management professionals are aware of the need to address this changing world. Their number one focus in the next one to three years is to proactively adapt to new risk types such as AI; geopolitical; reputation; environmental, social and governance (ESG); IT and cyber risk. Interestingly, the second-biggest priority is to leverage advanced analytics and AI for risk management.

Additionally, a vast majority (90 percent) of our survey respondents say that the pace of risk management transformation, fueled by technological disruptors, has increased, with 56 percent indicating that it has risen sharply. (Exhibit 2)

As risk functions grapple with these rising external risks and internal challenges, they are expected to be more productive and effective. They will also need to perform this work while reducing their overall costs and footprint and becoming more closely aligned with the strategic objectives and value-creation components of the business. Such a huge challenge will require greater collaboration across the organization.

Exhibit 2: Pace of risk transformation

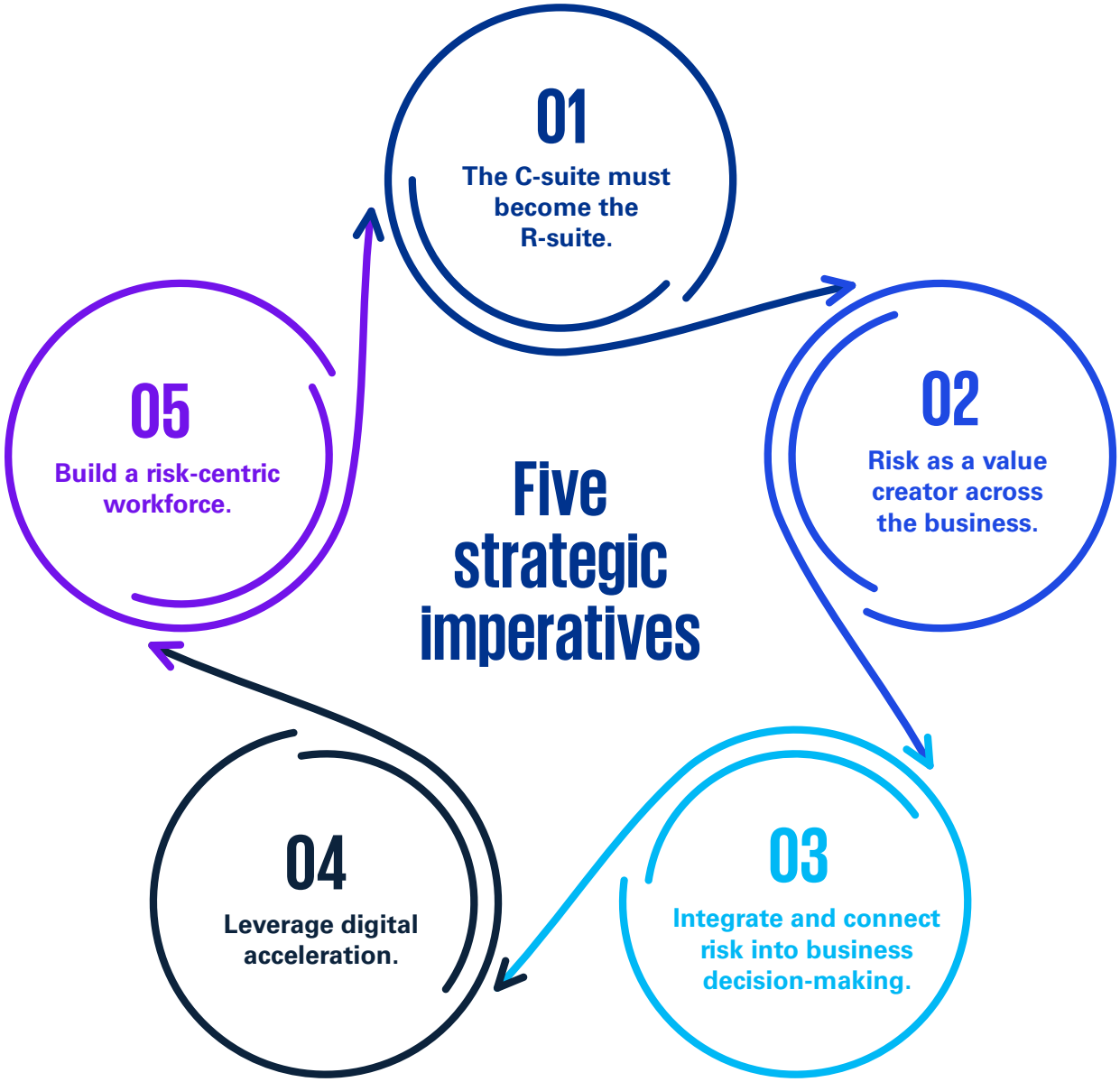


Source: KPMG International Survey, 2024

Five strategic imperatives for the risk function

Changing the formula for risk calls for a dramatic rethink in the way risk is managed. This process should include a greater role for other parts of the organization, more alignment and integration between risk and the business, and a need to perceive risk as adding value rather than simply avoiding damage.

We'll now examine the five strategic imperatives that businesses should focus on to successfully position their risk function to meet these future challenges.



1

The C-suite must become the R-suite

Risk is the business of every member of the C-suite. When asked how they can best help address external and internal drivers of risk, 76 percent of C-suite survey participants responded that they should lead by example by demonstrating a proactive approach to risk management, and 70 percent agree that they should develop and implement a comprehensive risk management strategy.

To meet these ambitions, chief risk officers (CROs) should spread risk ownership across the business. The increased importance of external risks — especially geopolitical — demands closer collaboration with business leaders to build risk into their strategy and business-as-usual.

C-suite executives should champion the changes required to restructure how the organization deals with risk and the ways staff incorporate risk into their decision-making.

Strong executive leadership is needed to shift employee attitudes and behaviors and to successfully integrate technology into the risk management process. Crucially, it will require a collective mindset from the top to achieve true team engagement across the executive ranks.

As the speed of change accelerates, 61 percent of executives surveyed inside and outside the risk function expect to see a significant increase in the level of risk they will be responsible for in the next three to five years — notably in operational risk, regulatory and compliance risk, and strategic risk (Exhibit 3). For C-suite executives taking part in the survey, the number one factor contributing to a successful risk transformation is leadership that fosters a risk-aware culture and prioritizes risk management throughout the organization.

61% of executives surveyed inside and outside the risk function expect to see a significant increase in the level of risk they will be responsible for in the next three to five years — notably in operational risk, regulatory and compliance risk, and strategic risk.

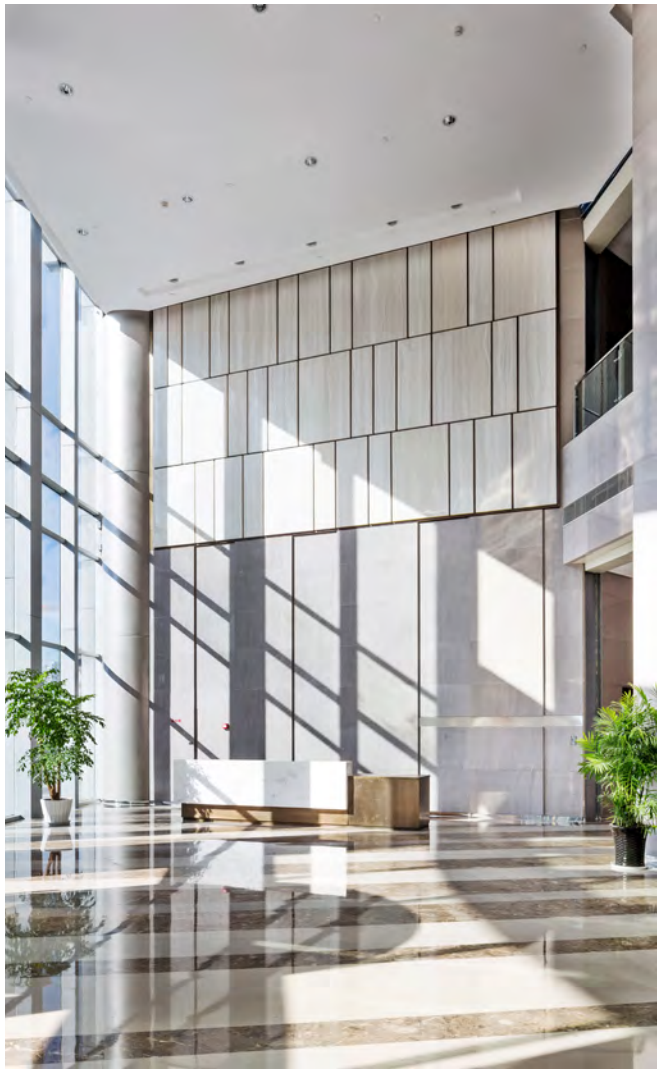
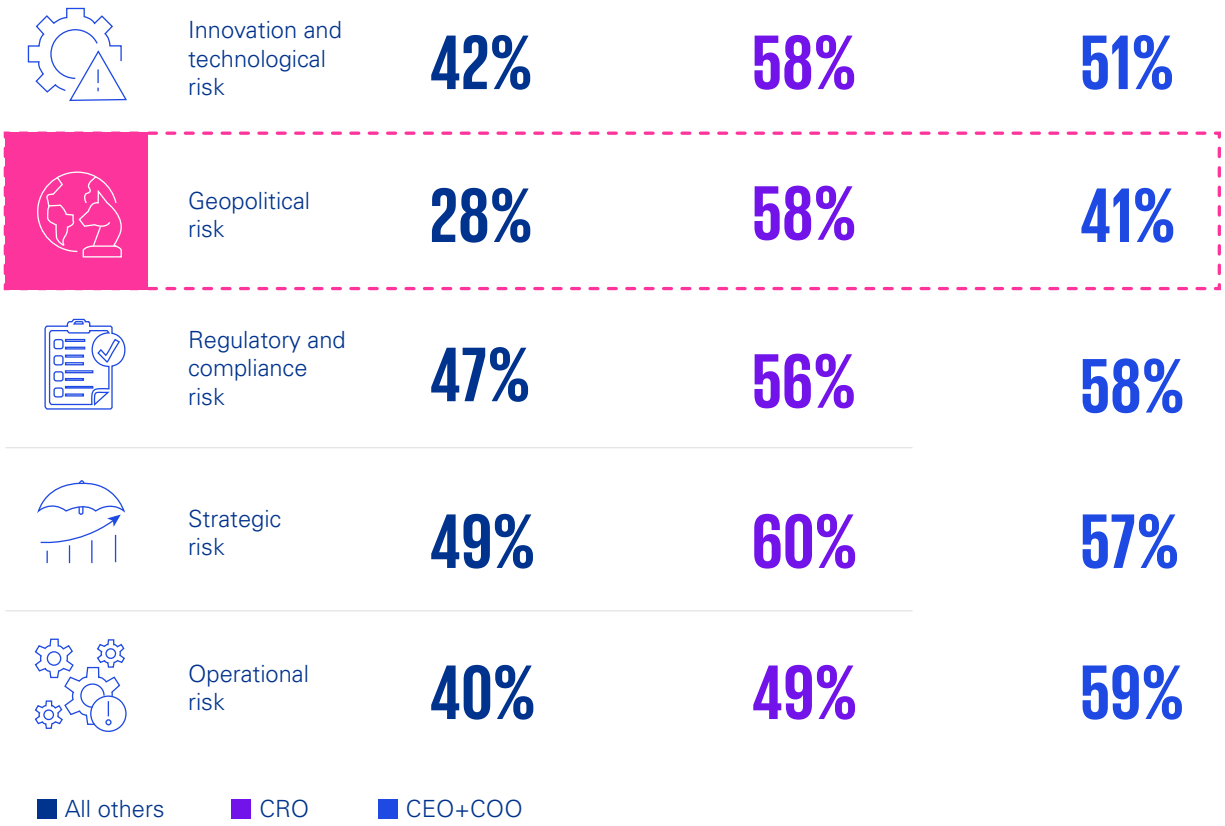


Exhibit 3: Functional view of current and anticipated risk categories to be overseen by leaders in the next three to five years



Geopolitical risk, although not among the highest priorities, is rising in importance. A consistent theme throughout the European Central Bank's May 2024 Financial Stability Review[1] is the idea that increasing geopolitical tensions and the instability they create can cause significant risk throughout the financial system. According to the group, "Continued geopolitical tensions pose the risk of economic and financial fragmentation in the world economy, with potential adverse effects on financial stability in the euro area and globally." It is likely that corporate leaders will be strongly focused on the results of various elections taking place across the world in 2024 — and the subsequent impact on their businesses. ESG risk is also becoming more of a concern in the wake of climate change and associated environmental disasters, which are disrupting supply chains.

[1] European Central Bank, "Financial Stability Review" (May 2024).

Key actions

Proactively address enterprise risks

C-suite executives should take a comprehensive view of the enterprise's needs and champion a process that drives wider enterprise risk management across all functions. This should increase organizational awareness of — and response to — contrasting and fast-changing risks.

Our survey shows that the main factor contributing to a successful risk transformation is to establish clear goals and take a proactive approach to addressing evolving risks. These objectives should be set by the people at the top, with the goal of cascading risk awareness and mitigation throughout the enterprise.

Empower leaders with data

The quality of executive decisions about risk depends on accurate, timely and comprehensive information. Data enablement should be a central part of the broader cultural change driven by the transformation of the risk function. That is crucial because if data is not up to the required standard, operations will suffer, with unreliable data quality continuing to impair the risk function's ability to inform key strategic and operational choices.

Our respondents underscore this concern: only 42 percent say data fragmentation and poor data quality can prevent effective decision-making and hamper collaboration. They add that it can create a lack of visibility into near-real-time information across business lines and an inability to calculate accurate measures of risk, and limit the ability to develop effective mitigation plans.

Build resilience

Resilience is a significant differentiator for today's top businesses. By developing the ability to anticipate, respond to and adapt to disruptive events, organizations can thrive in the face of adversity. Traditionally, resilience has been viewed as a qualitative attribute, often discussed in abstract terms such as adaptability, robustness and flexibility. However, to truly understand and enhance an organization's resilience, it is essential to also take a quantitative approach to resilience management — one that is data-driven and AI-enabled.

Quantitative enterprise resilience frameworks offer businesses a powerful tool to navigate today's unprecedented challenges. By leveraging advanced computational techniques, businesses can integrate various factors associated with resilience principles into a comprehensive model that supports decision-making in a complex and fast-changing world.

Case studies

Focusing on critical risks

Risks evolve at an alarming pace, and organizations must channel finite resources towards areas of highest impact. By rationalizing its risk frameworks, a financial services company has simplified its risk governance and policies, achieving more consistent risk assessments.

This process empowered the business to refine employees' accountability and responsibilities across the three lines of defense. It also put more decision-making power into the hands of the team, thus effectively spreading ownership across a larger group. The process of rationalization was extended to consolidate shared services, locations, and automation — with relevant C-suite members given more direct responsibility for risks in these areas. Not only does the company now have a clearer view of critical enterprise risks, it can also deploy a higher proportion of its staff towards these risks, becoming more cost-effective.

Getting on top of compliance

Compliance risk is a huge challenge, with a constant stream of new regulations impacting every part of the business. It is now a significant board-level issue that can leave companies vulnerable to potential rule breaches, heavy penalties, and reputational damage. Because of that, the C-suite must lean into this issue in ways that signal to others its importance and impact. For one large, US-based global technology company, the lack of a centralized compliance function led to inconsistencies and blind spots.

The company was inspired to rethink its entire compliance strategy and develop a global program, using technology to scan relevant regulations around the world. This was accompanied by training and communications to keep key decision-makers up to speed on compliance obligations and risks. Senior management can now cover all its regulatory bases and reduce any risk of non-compliance.

2

Risk as a value creator across the business

Key decisions by the risk function should begin and end by answering the question: how will this next step add value to the business? The actions of the risk team have an impact on the strategic, operational and financial value that the business generates. They also have a very direct impact on the ways in which the business is (and in some cases not) trusted. Given trust's essential value to all modern businesses, it must always be a part of the equation when it comes to assessing the value delivered to the business. And while risk management may remain at the heart of the function, it will need to be framed in terms of the value that it creates. Effective risk leaders can showcase the value they add by articulating their stories clearly and powerfully, linking their actions to corporate value.

Such an approach can help transform risk from the "department of no" to a service that consistently creates value — and that all employees embrace — and build a connective tissue with the C-Suite to help garner the support necessary to support risk transformation. In this way, everyone across the organization can be inspired to incorporate risk into their everyday decision-making.

But this process is a two-way street: those in the first line of defense should assume full responsibility for the risks of their actions, as well as the opportunities. The second and third lines can then devote their energies to focusing on their key priorities of compliance and internal audit without getting moved off target.

Faced with a rising tide of geopolitical, technological, ESG and reputational risks, the risk function cannot go it alone. To meet these challenges, survey respondents acknowledge the need to collaborate.

To better understand the likelihood and impact of large-scale events — and develop greater resiliency and agility, 66 percent of chief executive officers (CEOs) and chief operating officers (COOs) and 57 percent of CROs and risk managers point to a need for cross-functional task forces, collaboration and communication.

Technology can enhance collaboration and integration

Only **46%** of respondents rate the level of collaboration between risk domains as adequate. Technology, however, can enhance collaboration.

68% of respondents believe that integration and interconnection of risk management systems, domains and processes had a significant enhancement to effectiveness over risk-related decision-making.

Key actions

Develop a value-based risk framework

Risk leaders should help the business develop a value-based risk framework, enabling executives to model their strategic and operational decisions around risk — and the value they expect to gain from an improved understanding of risk. For instance, quantifying the impact of a cyber breach, supply chain disruption or damaging social media campaigns can focus executive minds on high-priority risks and allocate resources accordingly.

Understanding the value of different risks also enables businesses to evaluate the potential downside of key decisions like new product launches or outsourcing to cloud providers. In this way, the risk function becomes part of the value-creation process, enhancing its standing across the organization.

Reinforce the first line of defense

Leaders should also reinforce the use of the three lines of defense to enable the organization to manage risk more effectively. One way to accomplish that is to ensure that the first line of defense, the business units, embraces their responsibility for managing day-to-day risks in practice. This would encourage the second line (compliance functions, legal and enterprise risk management) and third line (independent assurance providers) to spend more time and resources on oversight, assurance, and planning for the possibility of "black-swan-style" big events and "unknown unknowns."

Define data requirements and reporting

When asked how risk data in leadership reporting has impacted decision-making, the number one response among CROs and risk professionals (67 percent) is an increased awareness and understanding of potential risks and their impact on the organization. But risk models can only be effective with the right data, which calls for clear data requirements.

For example, given the accelerating pace of climate change, it is imperative for companies to anticipate its far-reaching effects. To address this challenge, risk professionals should drive the development of sophisticated models that forecast the potential impact of global warming on businesses.

Use risk insights to educate the business

Part of the risk leader's role is to transplant the notion of risk into both strategy and everyday business conversations. To change risk perceptions, leaders should introduce common and straightforward ways to communicate risks, via dashboards and other visual tools. Once these tools and methods are consistently used and disseminated across the business, they should begin to become standardized and relied upon.

As business leaders drive these changes, their influential positions will propel these methods and help establish them as standard practices. When this happens, the enterprise will fully experience the positive impact of embracing risk.

Case study

Turning a business plan into a risk plan

To strengthen its market position in a niche sector, a wholesale bank acquired a relatively large, specialized bank. The entire transaction was approached from a business perspective, and the wholesale bank established a second transaction stream for the "regulatory takeover." The first step was to balance strategy with risks, determine capital and liquidity needs, and make a decision, with the business plan evolving into a risk plan and the entire transaction significantly influenced by regulatory considerations.

This need to implement regulatory requirements from day one created a sizeable operational project, involving management support from both banks to achieve compliance before the merger. The project owed its success to this effective combination of risk and strategic priorities, enabling the bank to align business and regulatory aspects to drive greater value to the enterprise.

3

Integrate and connect risk into business decision-making

Decisions affecting one office or department can have a ripple effect on all the others, and this applies to risk, too. A geopolitical event may disrupt supply chains, causing missed delivery deadlines, missed orders, and financial losses. A cyberattack on an organization may hamper its operations and seriously damage its reputation.

More than ever, this means that risk management should be effectively embedded in decision-making throughout the organization. Executives in our survey agree — saying the most sought-after objective of transformation is to build a comprehensive risk framework that integrates the identification, assessment, and mitigation of risk across functions. Other top goals are the alignment of the framework with business goals and efforts to make the organization more resilient. All of these objectives require the improved integration of risk with the rest of the business.

Sixty-five percent of C-suite executives — and 71 percent of CROs and risk managers — say that the integration of systems, domains, and processes can significantly enhance the effectiveness of risk-related decision-making.

Doing so should make it easier to identify potential risk-mitigation strategies, leading to greater consistency in managing enterprise-wide risk.

Regarding the integration of risk management data and resources across key business units, only 31 percent overall say this is occurring at a significant level. All sectors expect the level of integration to grow markedly in the next three to five years. For those in all sectors with a sizable level of integration, 84 percent in our survey say it has enhanced the effectiveness of planning and decision-making among business units.

Building trusted organizations requires an integrated platform that addresses every type of risk, with common data architecture and systems as an "ERP for risk," delivering a consistent view of risks. However, in most organizations, each function often has its unique risk system, which can lead to a complex, competing web of cloud-based and on-site systems. These systems are typically oriented towards specific risks relevant to a particular function. The result is inconsistent approaches to risk, along with significant "tech debt" costs of continually updating these various systems.

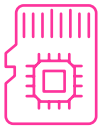
To make matters more complicated, some functional leaders are reluctant to move away from systems that they have grown accustomed to.

This issue should be addressed head-on because if multiple siloed risk systems continue to operate, the business will be unable to manage its overall enterprise risk.

71%

of CROs and risk managers — say that the integration of systems, domains and processes can significantly enhance the effectiveness of risk-related decision-making.

Key actions



Review the current risk technology landscape

Leaders aiming to reduce risks and increase agility should evaluate if their existing defense configuration requires modifications and determine the extent of changes required. This involves assessing technology and data capabilities against future risk management needs and then undertaking an inventory of the current systems, software and data products to identify needed changes across the entire enterprise.

During this review, risk and technology professionals should collaborate to establish a consistent risk technology landscape. This risk technology review should be holistic, examined using both a risk technology and enterprise technology lens. Technology governance should be assessed to ensure it aligns with both risk technology requirements and general technology governance principles. Technology and data capabilities should be evaluated to address the future requirements of risk management professionals, while integrating into broader architectural, technology design and governance frameworks. Finally, investments in risk technology should align with broader strategic business goals to deliver scalable, flexible technology that meets risk management needs and adapts to changing enterprise demands.

Align all stakeholders around single or fewer platforms and common systems governance

This is harder than you might think, with efforts to consolidate around one common platform likely to meet significant internal resistance, especially in financial services. It may be necessary to appoint a single executive leader to carry out this transformation, build a common architecture and solutions, and migrate functions to the platform.

One way to approach this problem would be to reduce working on shared platforms as much as possible. However, in some sectors — such as financial services — it may not be possible to create a single, enterprise-wide shared platform, as this would add enormous complexity and fail to accommodate diverse user needs.

An alternative approach would be to have a reduced number of platforms, but all operating off the same cloud, with common governance standards that define basic operating principles, enabling systems to interconnect seamlessly.

Modernize and optimize for impact

Once an integrated platform(s) is in place, risk management should be enhanced through managed services, tailored service delivery models, and automation to reduce "tech debt," cut down on manual tasks, and free up risk professionals to produce valuable insights for the business.

New GenAI enhanced technologies should be an integral part of these developments, processing a wider range of risk data from existing and new sources, and modeling scenarios, all at a significantly faster speed, to give near-real-time risk analyses.

Case studies

Integration builds trust

A large telecommunications firm faced significant challenges in achieving its goal of becoming the most trusted brand in its industry. The governance, risk and compliance (GRC) efforts of the 20 risk teams were hindered by a proliferation of legacy platforms, technology tools, siloed teams, disparate data sources and manual processes — with a lack of centralization and standardization. This fragmented landscape resulted in inaccuracies, delays, low visibility and a reactive approach to GRC. Leadership recognized the need for a massive transformation to centralize and standardize its GRC efforts, requiring a scalable and flexible platform with global reach and robust functionality.

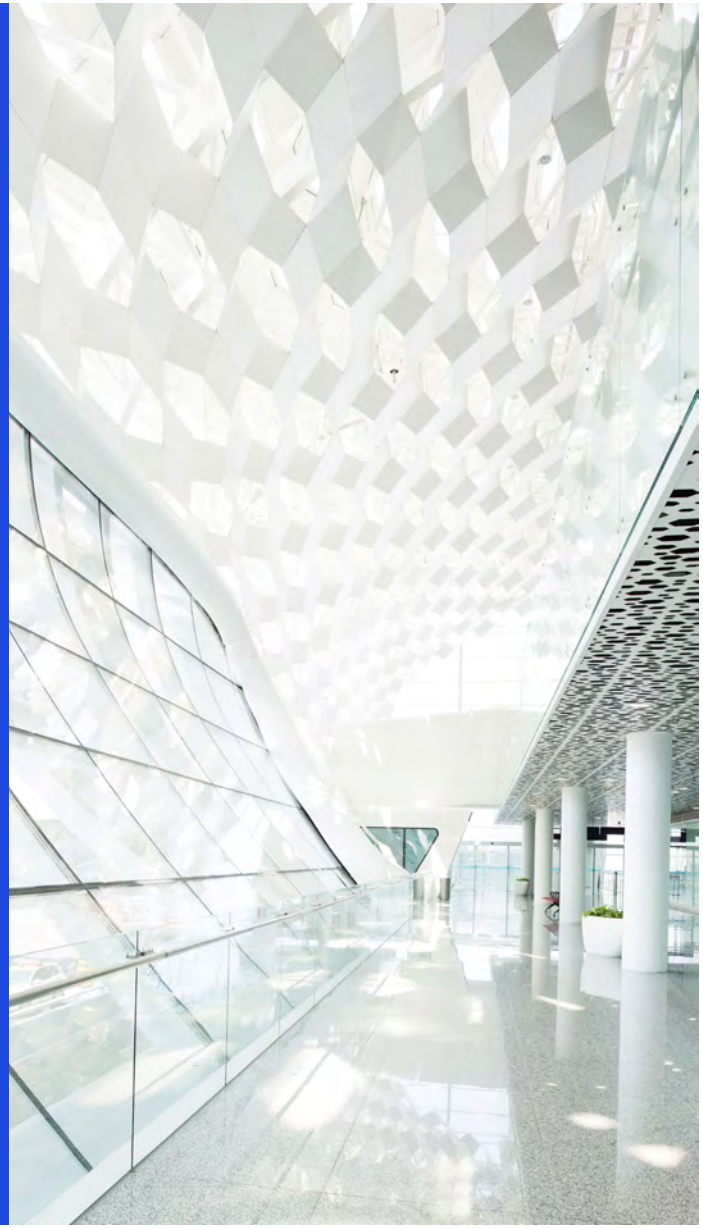
By moving towards this more structured approach, this business modernized its GRC functions, improved transparency and enhanced efficiency, setting a foundation for trust and compliance across the organization. Key outcomes included a centralized GRC platform serving 25 risk teams, increased stakeholder trust, an estimated 40 percent lower cycle times, and a more practical risk management culture.

Uniting for digital transformation

A major financial firm took on a formidable task. It sought to completely upgrade and modernize its IT core and business operations to meet future needs and address unanticipated risks while utilizing legacy data — all while embedding compliance obligations in a way that supported its digital transformation.

To accomplish this, the company developed and implemented an agile approach to compliance based on a deep understanding of regulatory requirements. This helped instill and build trust among the business's many stakeholders, including customers, regulators, employees and investors.

The result was a new digital infrastructure to help better serve its growing customer base; improved customer experience through better understanding individual customers and their journeys; and automation of compliance processes — linked to risk — that could be applied seamlessly to new products and markets.



4

Leverage digital acceleration and data analytics

Technological advances are accelerating, enabling risk professionals to manage change better — at the same time bringing fresh risks. The impact of new technology on risk management has been extremely positive: 98 percent of executives in our survey say digital acceleration has improved their organization's approach to risk, particularly in the fields of identification, monitoring and mitigation.

Encouraged by these results, organizations tell us they intend to invest more in technology. Forty-one percent surveyed are planning to spend more than half of their risk management budget on technology in the next 12 months, compared with just 28 percent in the previous year.

Innovative digital technology has been deployed across 54 percent of our respondents' organizations. And, according to CROs and risk managers, the biggest benefits of digital acceleration within the next three to five years are higher efficiency and cost reduction and streamlined monitoring using AI and ML models. Interestingly, CEOs and COOs ranked enhanced risk identification and data-driven strategy as their second highest priority (after AI and ML).

AI and GenAI can lead to automation across the enterprise, and the risk function is no exception. More than half of the executives we surveyed expect a reduction in the number of individuals working on risk, although more than a third do not foresee a decline, and seven percent are unsure. Fifty-nine percent of executives surveyed expect a reduction in the risk workforce.

AI, GenAI and other tools are neither job destroyers nor comprehensive solutions. They will work best when humans ask AI and GenAI the right questions and apply their judgment to shape the best answers. However, as organizations digitize and embrace AI, they should be seeking to gain trust in its application to avoid making important decisions based on false conclusions and to prevent data misuse that breaches privacy regulations. To accomplish this, risk professionals should bring technologies together in an integrated framework on a singular platform that uses common data and offers fast, easy-to-understand advice to users across the business.

98%

of executives in our survey say digital acceleration has improved their organization's approach to risk.

Key actions

Embed data-analytics

The early identification of emerging threats enables the organization to mitigate them and make better business decisions. Virtually all executives surveyed (90 percent) say their organization includes risk data in its reports to leaders. When asked about the ways this kind of reporting affects their ability to make decisions, almost two-thirds (65 percent) say that the inclusion of risk data has increased the awareness and understanding of potential risks and their impact on the organization. By contrast, the survey also shows that organizations that have not included risk data in reporting to their leadership have been prevented from doing so by a lack of appropriate risk data tools and difficulty in measuring their risk-management effectiveness.

Effective data analytics transforms increasing amounts of raw data into actionable insights, with with AI, GenAI and ML enhancing the ability to filter through data, spot trends and suggest solutions. More than three-quarters of the professionals we surveyed said they are using these technologies to streamline the risk process. And out of 16 options, executives chose AI and GenAI as by far the most popular type of technology for managing additional risk responsibilities in the next three to five years. It is also the most commonly identified solution that the risk function is planning to invest in over the next three to five years. And among those who use AI, GenAI and ML to improve risk operations, it was most frequently deployed for predictive analytics to identify potential risks.

Improve data quality

The quality of executive decisions depends on accurate, timely and comprehensive information feeding the insights. If data is not up to the required standard, operations will suffer, as our survey shows.

Variable data quality continues to impair the risk function's ability to analyze threats, with 42 percent saying that data fragmentation and poor data quality can prevent effective decision-making and hamper collaboration. They add that it can create a lack of visibility into near-real-time information across business lines and an inability to calculate accurate measures of risk and limit the ability to develop effective mitigation plans.

This is where a common data architecture and data governance can have the most positive impact, enabling everyone in the organization to feed in internal and external data, model risks, and gain a more accurate and up-to-date view of risks impacting their part of the business.

Place trust at the heart of AI usage

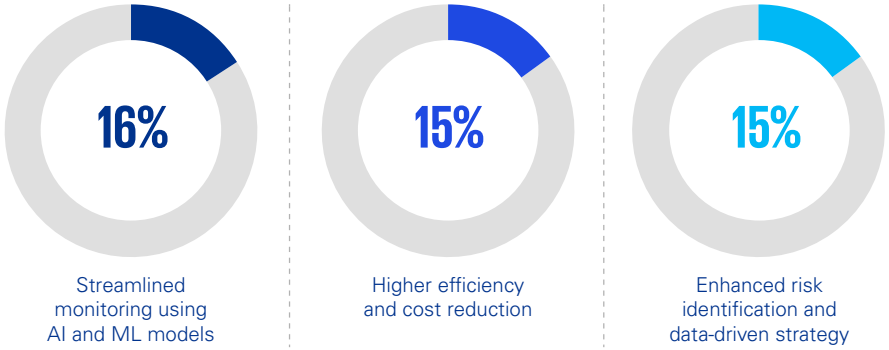
Regardless of the current state within each sector, all organizations need to take great care when deploying new technologies. Given the surge in resources flowing into AI and GenAI, organizations should invest wisely. In addition to investing in these technologies, businesses must remain focused on building out systems that resonate trust with both internal users and external consumers. If something goes wrong and that trust is questioned, it could harm the entire organization.

Decision-makers should approach AI and GenAI implementation in stages, testing areas where gains can be made fastest while ensuring that trust in the system is a constant concern. This way, AI and GenAI enablement can achieve quick wins while building an integrated and trusted platform over the longer term.

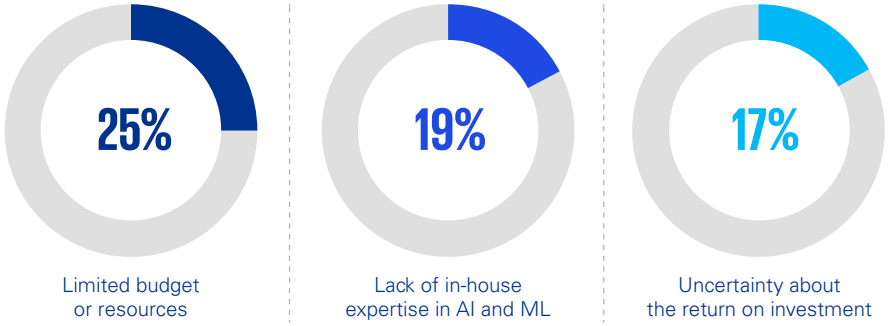
Leverage digital acceleration and data analytics

Seventy-eight percent of respondents report using AI and machine learning to streamline and improve risk management, including data analytics. That means the time to invest is now, before the chasm between late adopters and early adopters becomes a gulf.

Anticipated benefits of digital acceleration on risk management within three to five years



There are some factors that prevent organizations from implementing AI and ML:



For these organizations, looking to their ecosystem partners for workforce solutions and expertise can prevent them from falling behind.

Case studies

Unlocking regulatory risk insights with GenAI

This European bank wanted to explore the potential for GenAI in regulatory assessments to stay on top of and respond effectively to emerging reporting obligations. Its current processes were predominantly manual, making them slow and resource heavy.

The bank tested GenAI across a sample of 36 different regulations and found that the answers met users' expectations. Generative AI was able to swiftly summarize highly complex topics drawn from different regulations and highlight gaps in existing reporting. This approach is now being rolled out, which should lead to faster, more accurate responses at lower cost, and, ultimately, improved compliance.

Responsible AI governance

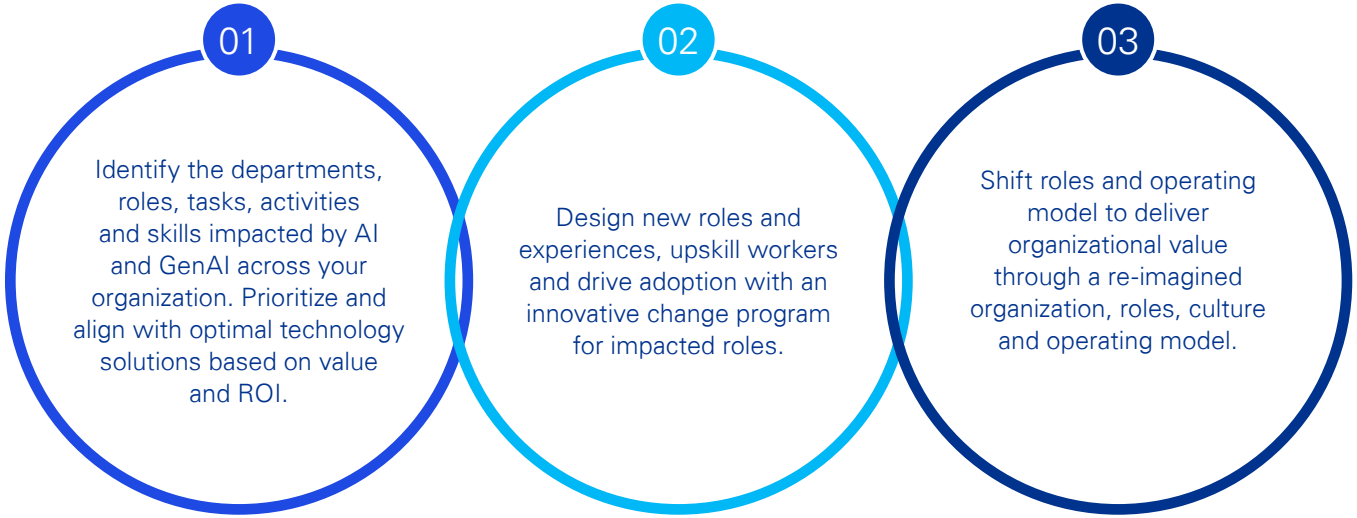
A global technology company was using AI and GenAI extensively but lacked a centralized inventory of the various AI applications. There were no clear responsibilities for addressing AI risk and no system for ranking AI risks to determine which ones were more important.

To address these shortcomings, the company assessed AI risk and impacts across various use cases. It recommended how to enhance and automate AI risk management, as well as how to compile an inventory of AI solutions and third-party services. The company now has defined roles and responsibilities for identifying and addressing AI risks, and a process for prioritizing these risks. All of this has made leadership more comfortable with the use of AI, giving a sense of greater control.

5

Build a risk-centric workforce

Innovative technologies, especially AI and GenAI, are vital to improve predictive capacity. But investments in this area should be accompanied by the development of a workforce with the skills needed to deploy them. It is crucial to understand that your investment in GenAI and the value it can create can only be captured when you also transform the people component of your organization. Accomplishing this requires a three-step process:



In their own ranks, over the next three to five years executives expect to supplement their risk management teams with expertise in three principal areas: IT risk, predictive modeling and cybersecurity skills. For C-suite executives, the top choice (45 percent) is optimizing cybersecurity measures, while for CROs and risk managers, the two biggest priorities are enhancing IT risk management strategies (36 percent) and integrating data analytics and predictive modeling.

Beyond these attributes, leaders are looking for people with interdisciplinary skills, especially in technology, innovation and industry-specific expertise. When asked about the expertise or perspectives they think multidisciplinary professionals can bring, both CEOs and COOs (51 percent) as well as CROs and risk managers (46 percent) agree that innovative problem-solving and strategic thinking are the number one benefits.

Key actions

Change the perception of the risk function from feared to trusted

In many businesses, risk itself has a serious reputation problem, typically viewed as the daunting and intimidating "office of no." As the C-suite moves to better embrace ERM, it needs to address legacy cultural aspects of the risk function to make the entire business a better risk partner. Businesses should reposition risk management through a change in mindset and training to shift to value creation, where risk becomes a form of resilience management. Changing that perception should make it considerably easier to properly integrate and get the most out of the risk function.

Our survey also reflects this: respondents said that fostering a risk-aware culture and prioritizing risk management throughout the organization is a primary factor contributing towards a successful risk transformation. Get this right and risk can become a trusted member of the C-suite that is known for delivering value.

Encourage self-reflection

Switching from a reactive to a proactive approach to risk may not come easily. Tomorrow's risk analysts should absorb insights and consider all the factors that influence the level of risk the organization faces. An ERM-oriented risk professional can look at issues like climate change, extreme weather events, geopolitical unrest and financial turbulence, and translate these into scenarios that inform the business front lines and help them adapt to build a resilient organization.

Invest in AI and cyber skills

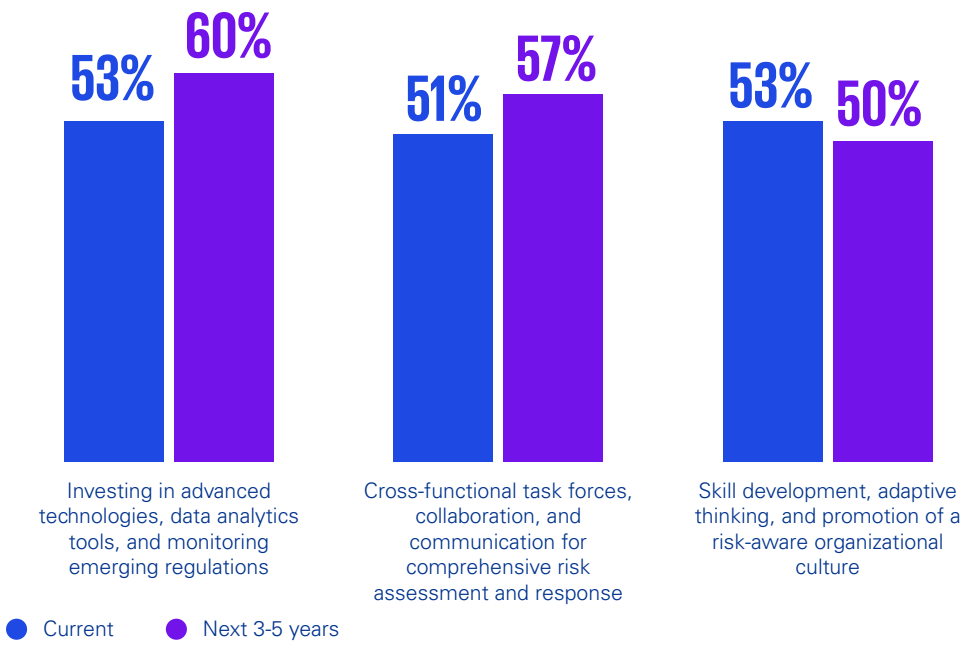
The increasing importance of technology calls for new skill sets for risk professionals. And these skills will not just be in areas like data science, data analytics, AI and GenAI, but also in change management, which will drive new ways of viewing enterprise risk and encourage greater awareness of emerging risks.

Automation powered by AI and GenAI can accelerate workforce reshaping, with a significant proportion of respondents saying this creates an opportunity to help staff develop skills for new roles.

Investing in skills, investing in people

Now and over the next three to five years, organizations are focusing on investing in tech and enabling cross-functional collaboration. However, while organizations are currently planning to implement workforce initiatives, we see that trend declining over three to five years, where three other top initiatives are set to rise.

Planned measures to improve the impact of large-scale events and develop greater resiliency and agility



What would improve collaboration between different risk domains?

- Increased training and education on collaborative risk management practices (59%)
- A culture that values and encourages teamwork and collaboration across different risk domains (41%)
- A governance structure that supports collaboration between distinct functions (41%)

Case studies

Embedding risk culture in a bank

Banks are under pressure to demonstrate "healthy" cultures with sound controls and good governance, where employees feel safe to speak up and challenge, and where rewards do not encourage irresponsible behavior. A global bank sought to build a stronger risk culture and worked to define and measure the appropriate underlying behaviors.

A pilot study was carried out in three business areas and four countries, surveying more than 5,000 employees and interviewing senior leaders. The bank now has a blueprint for a revitalized risk culture and has rolled out a methodology and operational model to consistently monitor its approach to risk and ensure it is aligned with its ambitions.

Closing capability gaps to manage technology risk

After implementing new technology, this organization needed to rethink how the first line of defense managed the associated risks. To do so, it defined its people's technology-risk capabilities and assessed to what extent leadership understood the risk management vision. The organization then refreshed the team's service offering and identified any skills gaps, developing learning pathways to address these gaps while also educating the leadership team to bring it in line with the risk ambitions.

Making risk less risky: Five steps towards transforming risk management

The risk universe is changing quickly and in unexpected directions, calling for nothing less than a transformation in how businesses perceive and manage risk. Above all, risk management's strategic imperatives should be closely in tune with those of the business and seen as part of everyone's brief to create a true enterprise risk framework and culture. Here is a brief roadmap to a future where risk management not only protects a business from uncertainty but also creates value.

1

Establish a risk vision

To initiate a more risk-aware culture, organize a workshop with the C-suite and key stakeholders, with the aim of making risk management a core, strategic capability. The workshop should articulate the impact of key threats, and establish a vision and some objectives, along with common, guiding principles for every function. This should set the tone for the transformation and get the entire executive team on board.

2

Develop an enterprise-wide risk management strategy

The risk strategy — which should align directly with the organization's strategic goals — outlines key risk areas and integrates risk management into business processes. It assesses the benefits to each part of the business in terms of creating value and preventing harm. To get started, form a cross-functional strategic risk planning group to conduct a high-level risk and value assessment.

3

Develop a communication plan

This plan should set out the objectives of risk management transformation, along with appropriate communication channels, to gain support across the C-suite and throughout the organization. The internal communications campaign should cover the first 30 days, followed by virtual 'town hall' meetings over the next 60 days.

4

Identify risk management skills and plan to fill any gaps

Once the skills have been "audited," the organization can start training and, in some cases, recruitment. A risk management mentorship program can stimulate interest in training and explain how risk impacts people in their daily jobs. Launch a skills survey within the next 30 days, and then partner with HR to develop an upskilling program within 90 days.

5

Create a data quality improvement plan

The aim is to enhance the accuracy, timeliness and completeness of risk management data by assessing and improving data governance, collection, storage and analysis. Start with a data quality audit across key business units within the next 30 days and followed by the formation of a Data Governance Committee within the next 45 days.

Study methodology

Our survey was conducted in February and March of 2024 and collected the responses of 400 senior executives in a range of functions, almost all of whom were C-level. More than half (218) are in risk management, and a slightly larger proportion lead the team managing risk at their company. Some 160 work at companies headquartered in North America, 126 in Europe, and 114 in China, Japan and Australia. The executives work in 11 sectors, with 80 or more in financial services, technology, and energy and natural resources. All the companies generate more than US$500 million a year in revenue and more than half of the executives work for companies with annual revenue of more than US$10 billion.

Explore our related content

KPMG Chief Risk Officer Survey

Explore CRO perspectives on their challenges, priorities and risk modernization trends

KPMG Chief Risk Officer Survey: Industry perspectives

Explore the CRO survey findings across the six industry sectors

Risk Modernization | Cut costs, not quality

Explore how to reduce spend without sacrificing quality of risk management outcomes

Risk modernization | Digital Acceleration

Explore the building blocks of digital acceleration and innovative technologies to transform Risk

Risk modernization | Implementing a modern technology architecture to accelerate risk transformation

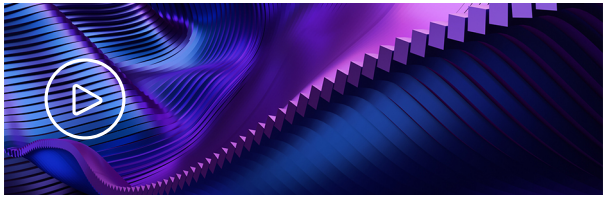
Position the risk function to be more proactive and a source of competitive advantage

Risk modernization | New ways of working in Risk

Embrace the future of risk management with transformative strategies in service delivery

Cybersecurity considerations 2024

Explore considerations that CISOs should prioritize to help build resilience



How risk and compliance can accelerate generative AI adoption

Quickly harness the power of generative AI in a trusted manner

KPMG Global CCO Survey

Explore CCO perspectives on their challenges, priorities and compliance modernization trends

How KPMG professionals can help

In navigating the intricate landscape of risk and compliance, organizations increasingly require robust risk management frameworks. KPMG risk professionals stand ready to assist, drawing upon extensive experience and technical capabilities to help you overcome multifaceted challenges. Whether grappling with regulatory complexities or evolving technology threats, KPMG firms offer a suite of services to fortify risk management practices and cultivate trust.

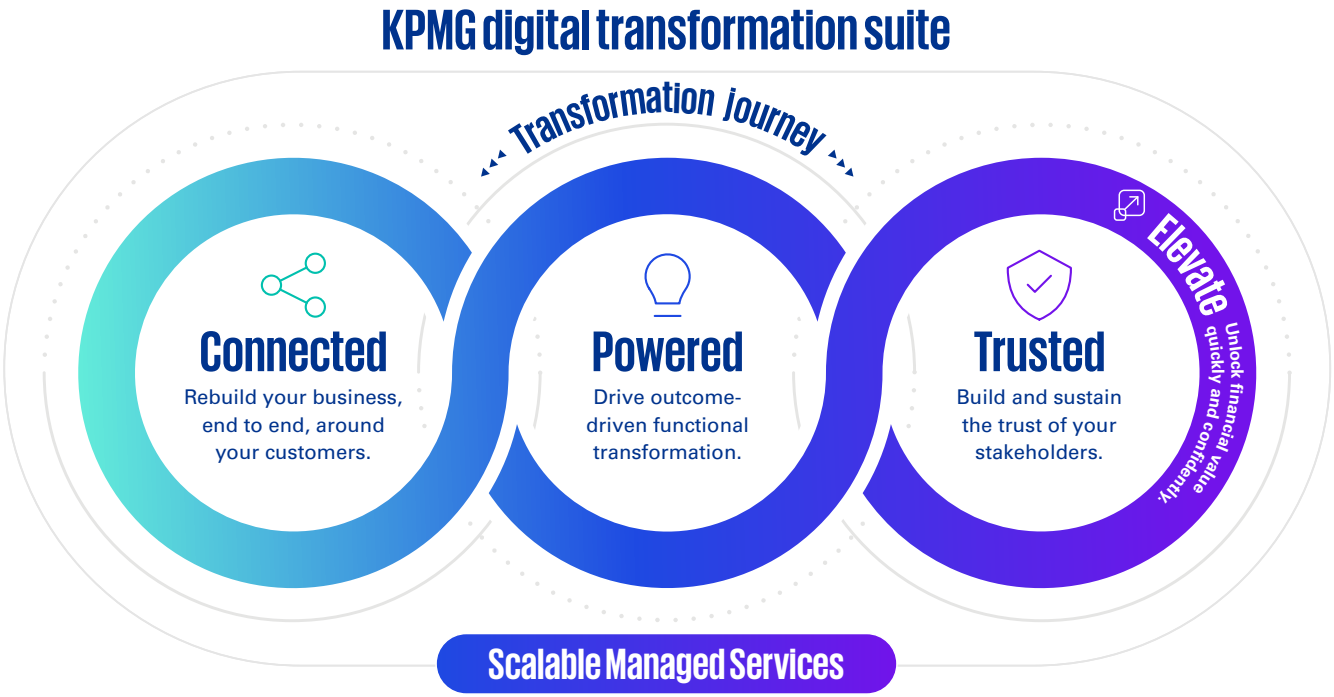
KPMG professionals merge their experience in risk with transformative insights to offer strategies that can not only shield against uncertainties but also illuminate new pathways to resilience, growth and building stakeholder trust. Leveraging powerful risk analytics, advanced modeling techniques, and real-time risk reporting, KPMG professionals empower organizations to integrate risk management into their daily operations. Through innovative services, we enable clients to proactively address emerging risks and seize opportunities for value creation.

Our services-driven approach is tailored to meet evolving business needs, with the aim of ensuring that risk management remains adaptable and responsive. By collaboratively building robust risk programs, KPMG professionals can help organizations cultivate trust with stakeholders while navigating the dynamic business landscape with confidence.

In addition, KPMG firms' suite of business transformation technology solutions can help you engineer a different future — of new opportunities that are designed to create and protect value. From strategy to implementation, KPMG professionals can help make the difference on your transformation journey. Together, we can help transform your current business model to reduce risks and drive future competitiveness, growth and value.

KPMG. Make the Difference.

Learn more at: visit.kpmg.us/RiskServices



Contacts

Tim Phelps
Risk Services Leader
KPMG US
E: tgphelps@kpmg.com

Brian Hart
Offerings Leader, Regulatory and Compliance
KPMG US
E: bhart@kpmg.com

Kyle Kappel
Offerings Leader, Cybersecurity & Technology Risk
KPMG US
E: kylekappel@kpmg.com

Ric Kimball
Offerings Leader, Internal Audit & Controls
KPMG US
E: ekimball@kpmg.com

Matthew McFillin
Offerings Leader, Forensic Services
KPMG US
E: mmcfillin@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**