KPMG Risk and Resilience Survey

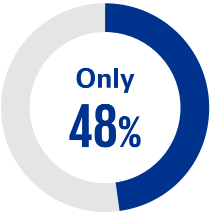
When “good enough” is not enough: The state of risk management and resilience

Introduction

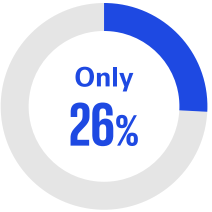
Emerging risks and threats to resiliency are rapidly growing in number, size, scope, and severity throughout the business world. Leaders are highly concerned about cybersecurity, data privacy, geopolitical issues, environmental threats, financial volatility, and other major risks. They also understand the vital importance of maintaining resilience in the face of disruption, system failures, and operational shutdowns.

This raises a critical question: How are US organizations managing risk as well as maintaining security and resilience in this fast-moving, volatile, and unpredictable environment?

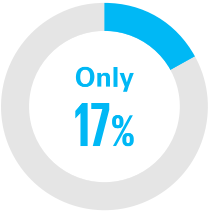
The 2025 KPMG Risk and Resilience Survey suggests that for many organizations, the ability to manage threats and disruption is a work-in-progress. **Consider these findings:**



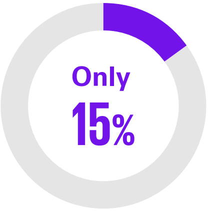
of organizations in the survey have a centralized structure for managing risk and resilience.



have a cross-functional view of risks.



have extended resiliency plans beyond critical processes.



are heavily reliant on advanced analytics for risk management.

Now is not the time for half measures and "good enough" initiatives. In a modern business environment marked by unprecedented levels of volatility and rapid change, organizations must adapt. According to a recent KPMG survey, 61 percent of executives expect to see a significant increase in the level of risk they will be responsible for managing in the next three to five years.[1] In another KPMG survey, 67 percent of CEOs said they are currently making significant strategic adjustments in response to geopolitical uncertainty, wars, conflicts and major elections around the world.[2]

In this new era of volatility, how well organizations manage risk and further their resilience capabilities will separate the winners from the losers. We believe that only those organizations that build resilience capabilities that adapt to tackle these uncertainties and volatility will achieve long-term success.

> **Our survey findings highlight a significant gap between leaders' recognition of the need for enhanced resilience and the implementation of effective measures to handle broader disruptions."**
>
> **Joey Gyengo**
> US Enterprise Risk Management Leader
> KPMG LLP

[1] Future of Risk, KPMG LLP, 2024

[2] 2024 KPMG U.S. CEO Outlook, KPMG LLP, 2024

This research points to what is working. Respondent organizations are achieving better risk management results with common, enterprise frameworks and supporting capabilities aligned to business strategy, deep integration across business functions, enabled on a technology infrastructure for faster, effective response to uncertainties.

In most organizations, risk management continues to be reactive, focused primarily on identifying and mitigating specific risks, offering little visibility or agility to manage their impact. In contrast, organizations with effective organizational resilience incorporate multiple risk disciplines, such as enterprise risk management (ERM), cybersecurity defenses, business continuity playbooks, and technology risk planning that is continuous and preemptive. These integrated teams and capabilities strengthen the organization's ability to anticipate potential disruptions and design strategies that will adapt and thrive in the face of adversity. And when crisis strikes, these same companies are best designed and prepared to respond.

In the pages that follow, readers will learn more about key findings from the KPMG 2025 Risk and Resilience Survey. This includes how organizations are structuring their approaches, integrating risk and resilience management into strategic planning, and leveraging tools and modern technologies to increase the effectiveness of their risk and resiliency processes. We also share several practical recommendations for enhancing risk and resilience management in your own organizations.

[1] "2024 KPMG CEO Outlook," KPMG, 2024.

[2] "AI Q4 Pulse Survey: Key Findings," KPMG, Q4 2024.

About the survey

Methodology

The KPMG Risk and Resilience Survey was conducted online in the US in November 2024. Respondents included 208 C-suite leaders including chief risk officers (CROs), chief technology officers (CTOs), and chief financial officers (CFOs).

The respondents served in large enterprises with at least

1,000

employees and an annual revenue of at least

$4 billion

Financial services organizations reported at least

$25 billion

in company assets.

A mix of industries were represented in the survey, including: energy, natural resources, and chemicals; healthcare and life sciences; technology; consumer and retail; industrial and manufacturing; telecommunications and media; fintech; media and entertainment; and financial services for insurance and banking.

Objective

The objective was to gather insight from C-suite leaders regarding the management of risk and resilience within their organizations. This included understanding how organizations structure their approaches and integrate risk and resilience management into strategic planning and business functions. The survey also examined how organizations leverage technology, data, and reporting to increase the effectiveness of their risk and resiliency processes.

Definitions

Before going through the survey, respondents reviewed the following definitions:

Risk is the possibility that events may occur and affect the achievement of strategy and business objectives.

Risk management aims to identify, analyze, and mitigate risks to achieve strategy and business objectives, thereby maximizing the upside and minimizing the downside.

Resilience aims to withstand and recover from disruptions or setbacks.

Building the resilient enterprise

Key findings and insights

The survey reveals that there is a significant gap between the recognition of the need for improved risk and resilience management and the implementation of those same effective measures. Company leaders are increasingly aware of the benefit of better resilience. However, articulating this need does not lead to proportional progress and investment for many survey participants.

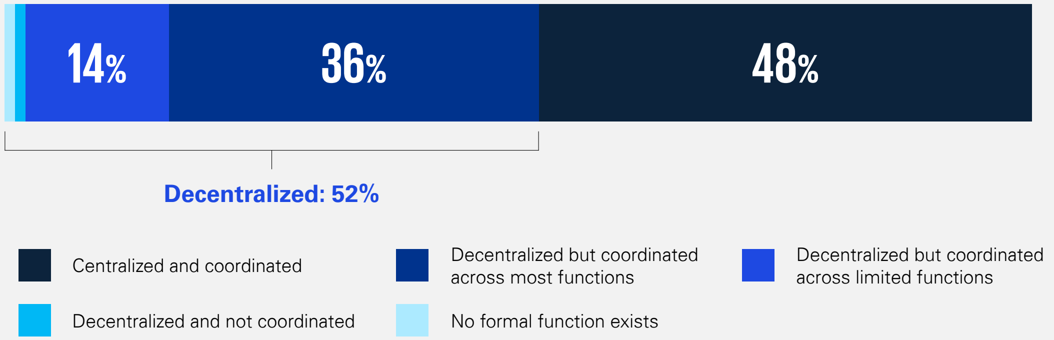
Another key finding is that organizations with centralized risk and resiliency management structures have made greater strides in coverage and capabilities, leading to improved performance for risk mitigation and enhanced resilience. Simply put, decentralization of risk and resilience management is not an optimal solution. In fact, strong risk management functions that are not connected or tightly integrated are prone to gaps in coverage or exploitation—intentional or otherwise. Enhanced performance is driven by fewer barriers to managing risk, a greater focus on tracking emerging risks, better integration, and stronger confidence that their C-suite leaders understand business risks.

We also observed that organizations without a recent major incident or significant downtime tend to limit investment in risk and resilience. Some adopt in-between measures or fail to integrate various functional insights into the organization's operations, from strategic planning to board reporting. While risk management tends to be partially developed, particularly in certain risk domains, resiliency lags in maturity and is not fully embedded in the strategies, processes, and ways of working. Many of the same insights gathered for risk management are not aggregated or shared in a way that supports business resiliency, including rapid response and recovery.

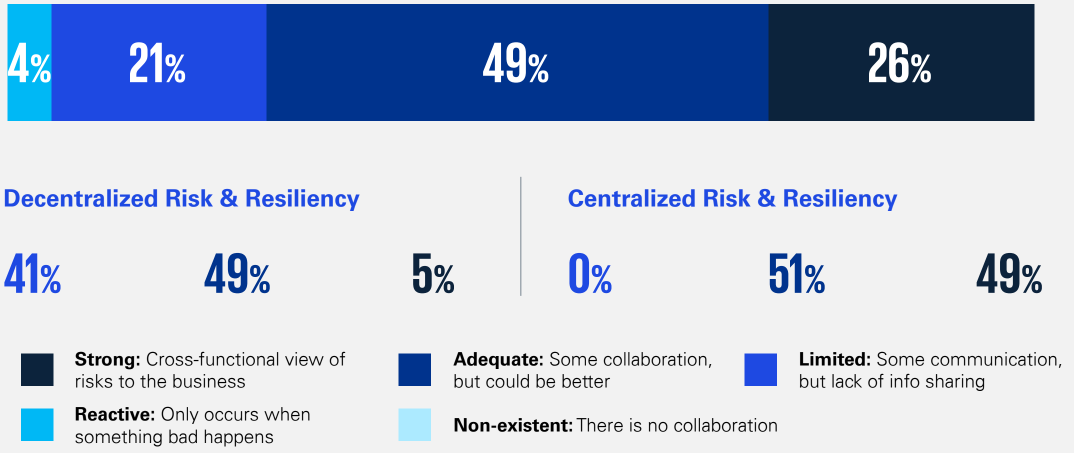
Centralized or integrated risk and resilience structures drive performance

Just over a third (36 percent) of organizations that take a decentralized approach to managing risk and resilience coordinate across most functions. More than half, 52 percent, of US organizations have not integrated risk and resilience capabilities, accountabilities, or organizational structures. Only 26 percent of organizations have strong, cross-functional collaboration, while 49 percent think collaboration could be better.

Organization Structure for Managing Risk and Resilience



Collaboration of Risk Management across Business Functions (finance, IT, operations)



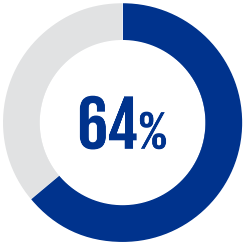
Decentralization of risk and resilience leadership does not result in better risk and resilience management. Having an integrated risk and resilience strategy, governance, process, and technology does.

If organizations do not start integrating and aggregating risk information consistently and sharing across relevant stakeholders groups, then those organizations will continue to be surprised by risk events and will need to respond more frequently to crises.

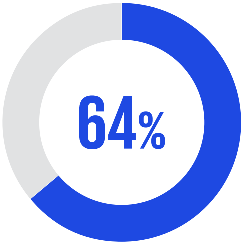
In many cases, a risk and resilience management structure might be "built," but often does not work effectively across business functions. In addition, resilience (58 percent) trails behind risk management (64 percent) when it comes to being fully integrated with individual business function and strategic planning.

In summary, organizations that are integrated and work together in a collaborative, cross-functional way appear to have strengthened the coverage, tightened the attack surface, and have more effective risk management and organizational resiliency.

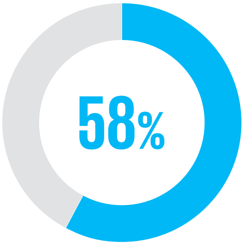
Degree to which risk management and resilience are integrated into strategic planning and business functions



Risk & resilience integrated into all of organization's strategic decisions and planning



Risk management integrated into the decision-making process of individual business functions



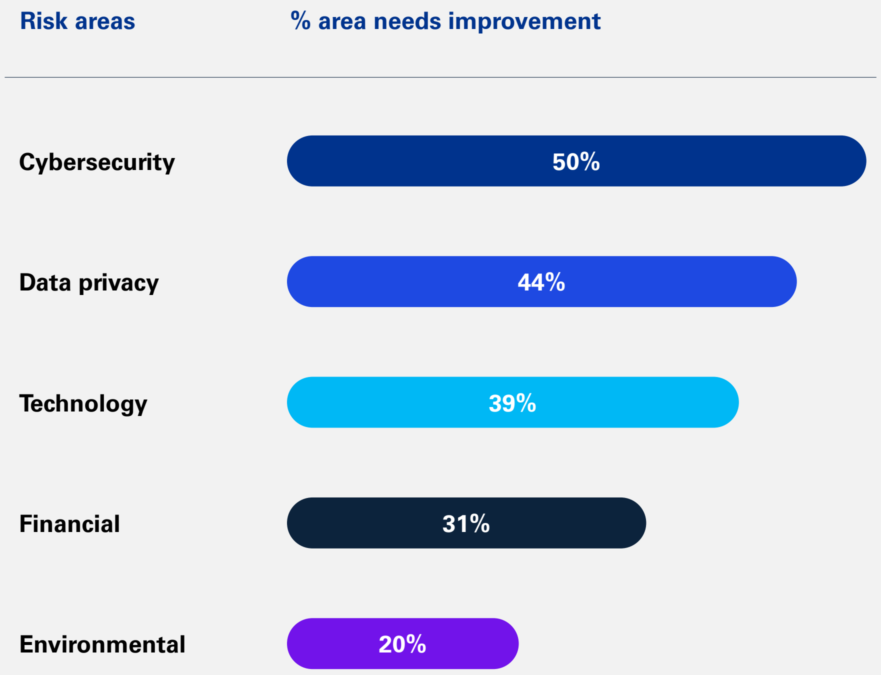
Resilience is integrated into the decision-making process of individual business functions

Bigger risk areas need bolder and smarter approaches

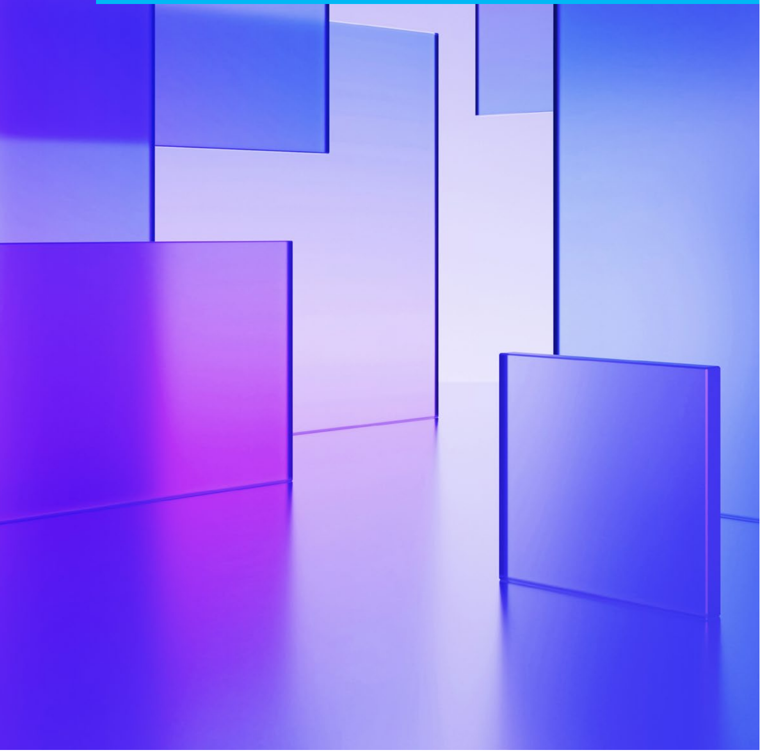
In our findings, cybersecurity continues to be considered the top risk for businesses over the next five years at 57 percent, followed by data privacy risk at 43 percent and technology risk at 41 percent. Each of these top risks is a critical consideration for strong risk and resilience programs and is perceived as needing improvement as the chart shows below.

Top risk areas that need improvement

Bigger risk areas need bolder and smarter approaches that are more integrated and effective than simply weaving together mitigations into consolidated reporting.



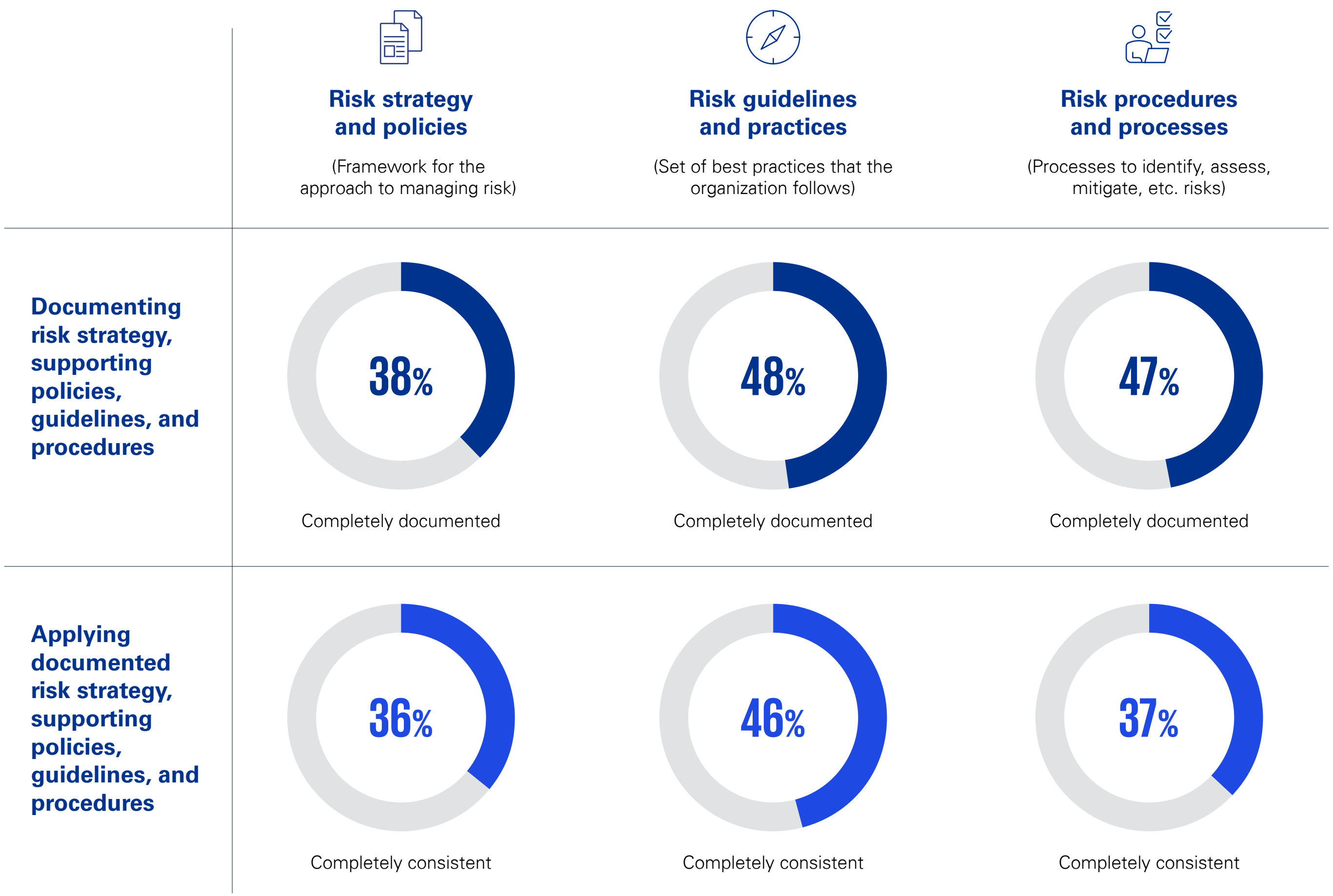
The successful application of risk strategies requires fostering a culture that rewards accountability for risk-taking, clarity through specific policies and guidelines, and cross-stakeholder engagement in matters that impact the company's well-being.



Executives surveyed say programs are being established to identify and document risk, but real-world application lags. Organizations are further along in "completely" documenting risk guidelines (48 percent) and procedures (47 percent) than they are with their risk strategy documentation (38 percent). Only about half of respondents indicated their efforts are "somewhat consistent" in the application of these strategies.

Documentation is not the answer, but it is part of the answer. More importantly, leaders are starting to have the right conversations and asking the right questions: What's most critical? What drives revenue? What would impact our reputation? What would shut us down?

Documenting vs. applying risk management and resilience strategies



	Risk strategy and policies (Framework for the approach to managing risk)	**Risk guidelines and practices** (Set of best practices that the organization follows)	**Risk procedures and processes** (Processes to identify, assess, mitigate, etc. risks)
Documenting risk strategy, supporting policies, guidelines, and procedures	38% Completely documented	48% Completely documented	47% Completely documented
Applying documented risk strategy, supporting policies, guidelines, and procedures	36% Completely consistent	46% Completely consistent	37% Completely consistent

Growing use of specialized technology, AI, and advanced analytics increases resiliency

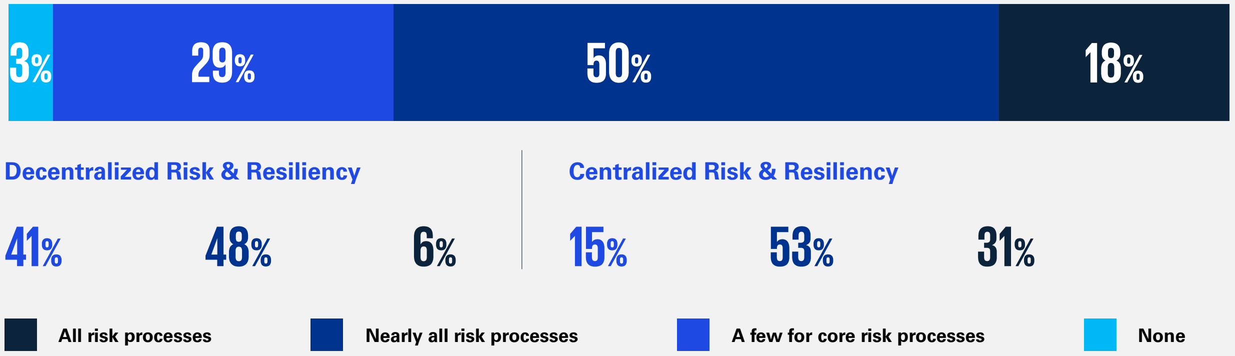
> Tools alone do not address potential risks or resilience challenges, but having an intentional technology strategy that aligns with the organization's mission can help them determine and respond to threats faster.

Organizations need a set of fit-for-purpose toolsets enabled by an outcomes-based technology strategy to support effective risk and resilience management. In addition, the data required to actively manage risks and improve resilience capabilities needs to be accurate, up-to-date, and easily accessible.

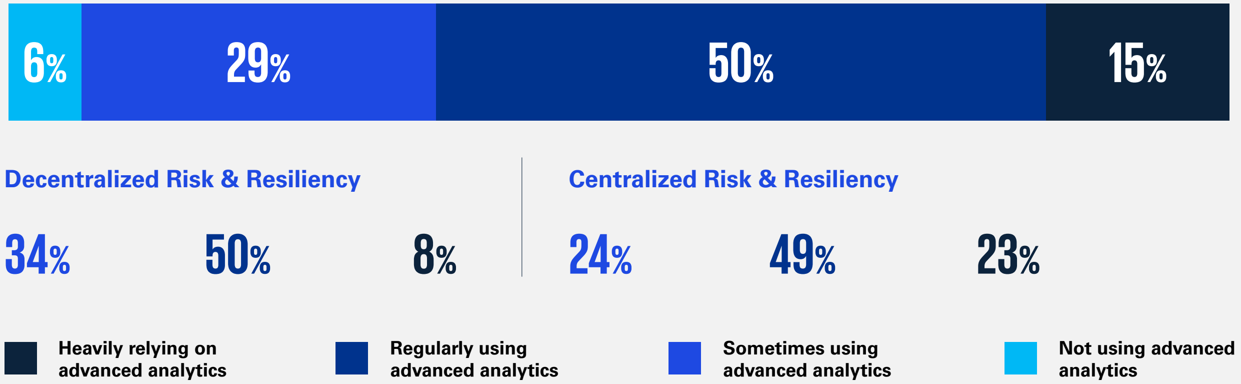
According to the survey, the use of specialized technology, AI, and advanced analytics for tasks such as governance, risk, and compliance (GRC) management, risk monitoring, and risk reporting is fairly common, with two-thirds of respondents relying on them to manage all (18 percent) or nearly all (50 percent) of their risk processes to identify, assess, monitor, and mitigate risks.

Risk and resilience management today is equally complex given the volatility of IT environments, but the data required to actively manage risks and improve resilience capabilities is readily accessible. By leveraging a modern, data-oriented approach backed by AI and analytics technologies, organizations can have trends and insights readily available to make critical decisions.

Collaboration of risk management across business functions (finance, IT, operations)



Use of advanced analytics to manage risks



Stakeholders expect leaders to take greater accountability for risk and resilience

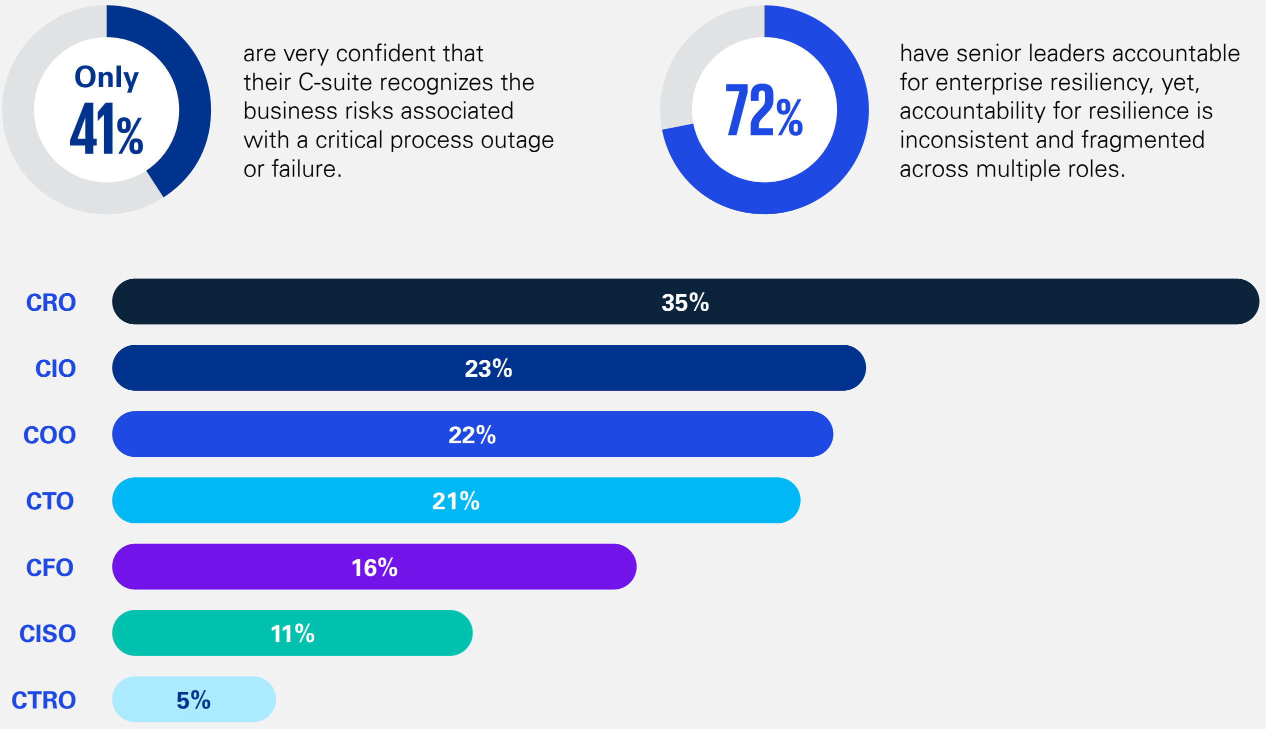
A culture of continuous engagement is essential, where the C-suite understands and plans for the business impact of critical process failures and builds resilience into all people, process, and technology investments. However, only 41 percent of executives are very confident that C-suite leaders understand potential risks and what's at stake. Conversely, risk executives may also be falling short in delivering risk insights that focus on time, attention, and funding.

About three-quarters (72 percent) of organizations have senior leadership accountable for enterprise resiliency. However, responsibility for resilience is not consistent. Ownership is spread across multiple roles, essentially resulting in a very fragmented or diverse approach to this challenge. A third (35 percent) of organizations rely on their CRO, but this responsibility also falls to other C-suite roles such as CIOs, COOs, CTOs, CFOs, CISOs, and CTROs. Twenty-five percent have no senior leader responsible for resilience.

> **Earning support for an integrated risk and resilience program requires a clear problem statement, cohesive strategy, and alignment of multiple stakeholders.**

Growth does not happen by playing it safe, and no organization wants to stall its growth. Support for an integrated risk and resilience program requires a cohesive strategy across multiple business functions, backed by continued investment in a unified governance model, educating or hiring qualified resources, optimizing or streamlining processes, and deploying leading technologies to orchestrate them. Equally important, leaders should empower their employees to take meaningful risks that ensures versus jeopardizes the resilience of the organization or processes.

Senior level leaders accountable for enterprise resiliency



Only 41% are very confident that their C-suite recognizes the business risks associated with a critical process outage or failure.

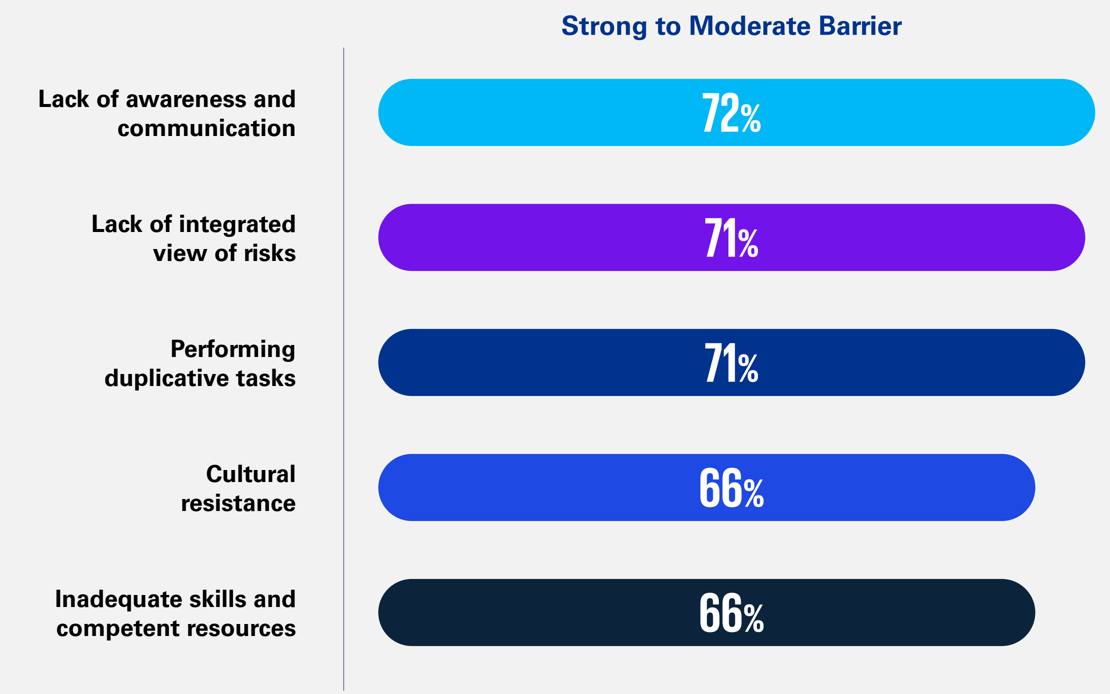
72% have senior leaders accountable for enterprise resiliency, yet, accountability for resilience is inconsistent and fragmented across multiple roles.

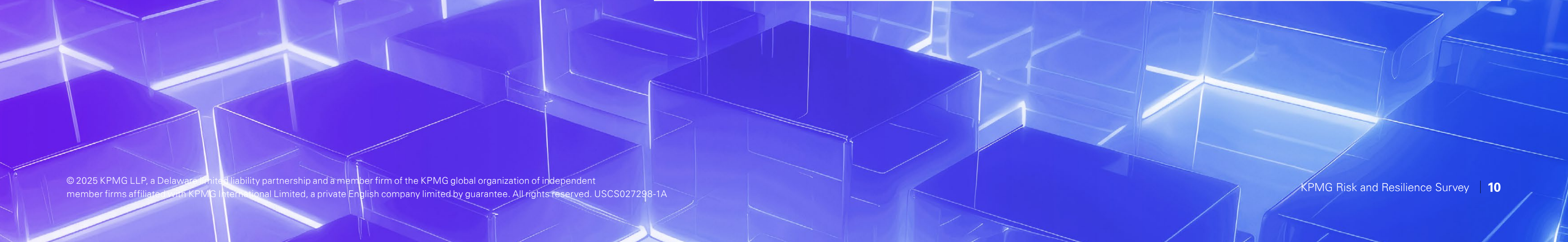
Organizations still face significant barriers to effective risk management

In the survey, two-thirds (66 percent) to nearly three-quarters (72 percent) of organizations face moderate or strong barriers to effectively managing risk. In addition, respondents do not believe that their organization is achieving a proper balance of risk exposure versus risk reduction based on current spending levels. Often, leaders can overcome these barriers by creating partnerships within the organization and transparency into the risk exposure of the company, improving the quality and comprehensiveness of risk management, and the areas that need to be addressed to enhance organizational resilience.

> **Barriers to managing risk are usually not about employees who do not want to do the right things—it is often due to the lack of integrated risk insights coupled with siloed communication and transparency that discourages intelligent risk-taking.**

Barriers to effectively managing risk at organization





Where to go from here

The landscape of risk is evolving rapidly and in unpredictable ways, necessitating a fundamental shift in how companies approach risk management and resilience. Most importantly, the strategic priorities of risk management must align closely with the overall business goals and should be integrated into everyone's responsibilities to foster resiliency.

Here are steps business leaders can take to make their organizations more resilient and drive value creation:

1 Gain leadership alignment to establish a centralized and integrated approach to risk management and resilience

The foundational step is to establish a centralized and integrated risk and resiliency structure. This applies to all industries. Organizations with a single view of risk perform better in tracking emerging risks, experience fewer barriers, maintain more advanced capabilities, and gain stronger confidence in the C-suite's understanding of business risks.

This is not to say that organizations should adopt a strict "command and control" approach. Assuming there is trust, transparency, and stakeholder alignment with the organization's overall mission, an effective approach can be to build advocates through a hub-and-spoke model instead of investing in point solutions scattered across multiple business functions that do not talk to each other or are complex to collaborate.

Accordingly, establish or expand the remit of risk management committees that include representatives from all major business functions—including technology and cybersecurity—to ensure cohesive and well-informed decision-making.

Make it clear that senior leaders need to be fully accountable for the success of risk and resiliency programs.

Currently, only 41 percent of organizations are very confident in their C-suite's understanding about risk and resilience, but a culture of continuous engagement is essential. The C-suite needs to understand and plan for business impacts of critical process failures and building resilience into critical technology investments.

Falling behind can be costly to an organization and result in the business losing competitive advantage.

2 Enhance resilience through cross-functional collaboration and risk management strategy integration

With a strong foundation in place, organizations can promote cross-functional collaboration in managing risks. Strong collaboration across departments with transparency into risks is crucial, as noted by 49 percent of organizations aiming to improve in this area. This will foster greater synergy and alignment in your risk management efforts.

Fully integrate risk and resilience considerations into both strategic planning and individual business functions—such as sales, marketing, supply chain, finance, IT, and operations—with a priority on critical business functions. Our survey indicates that while 64 percent of organizations have integrated risk management into their business strategy and planning, resilience integration lags behind at 58 percent.

Achieve mature integration amongst key risk management groups (e.g., cybersecurity, business continuity, third party, and ERM programs) to collectively manage risks as part of the broader risk management framework.

THROUGH THE ERM LENS

ERM: The glue that integrates risk and resilience

ERM has the opportunity to significantly enhance organizational resilience. Its capabilities are both critical and pivotal to fostering resilience, acting as the glue that unifies various risk functions. ERM's unique perspective allows for comprehensive risk identification and assessment, the development of mitigation strategies, and coordinated incident response. By promoting collaboration among different functions, ERM ensures that risk and resilience strategies are robust, aligned, and continuously improved.

THROUGH THE CYBER LENS

Strategic cyber resilience

In today's rapidly evolving threat landscape, Chief Information Security Officers (CISOs) must embrace a "resilience by design" mindset, as emphasized in the KPMG Cyber Considerations 2025 report.[3] This approach involves not only maintaining a comprehensive view of the organization's security posture but also efficiently identifying, managing, and monitoring critical assets and supply chain participants. As digital transformation initiatives mature, the convergence of AI adoption, reliance on a hybrid workforce, and the expansion of supply chains introduces significant cracks in the attack surface. CISOs must ensure their strategies are robust and adaptive to these evolving challenges to enable the organizations to be trusted entities.

3 Invest in technology to take decision-making to the next level and improve outcomes

Use specialized technology, data, advanced analytics and other emerging tools to manage risk and resilience processes. Organizations do not always fully integrate them with other data sources and data destinations. For example, the right cybersecurity tools used in the right way can scan networks on-premise and cloud applications for a wide range of vulnerabilities, helping to identify potential weaknesses that could be exploited by cybercriminals or lead to operational disruptions. These tools can also be used to analyze large datasets, helping to reveal patterns and trends that indicate potential risks such as fraud, operational inefficiencies, or security breaches.

Aim to fully automate risk management processes. While two-thirds of organizations in the survey have mostly automated their processes, only 11 percent have achieved full automation. Automation will enable transparency of risk, leading to faster decision-making based on insights.

Automated risk management processes, coupled with AI and advanced analytics—such as predictive modeling, scenario analysis, and monitoring and sensing—supports a more robust approach to risk management. This enables different stakeholders to look at the same data and generate function-specific insights to foster better decision-making. Further, this allows for better anticipation and mitigation of emerging risks. Half of the organizations in the survey regularly rely on advanced analytics, but only 15 percent heavily rely on it.

Ensure that data used in risk reporting is of high quality, is as complete as possible, and is up to date. Data should be drawn from different risk areas to provide a comprehensive view of the risk landscape. Incorporate additional assessments and scans performed throughout the organization—such as business impact, IT risk, and IT application assessments—for a thorough, data-driven approach.

4 Get the insights you need with integrated data sources

Integrate external data sources like market trends and industry benchmarks into your risk analysis procedures. Sixty-eight percent of organizations frequently leverage external data. Doing so will help ensure that your risk perspectives are comprehensive and well-grounded.

Integrating comprehensive data sources, both internal and external, is critical for effective risk management as it supports a view of potential threats and opportunities. Internal data offers insights into organizational processes, historical performance, and known vulnerabilities, while external data enriches this view with information on market trends, regulatory changes, emerging threats, and competitive dynamics. Together, they enable more accurate risk assessments, predictive analytics, and proactive risk and resilience strategies.

Collaborate with industry bodies, government agencies, academia, consultancies, and/or third-party data providers to support data-driven insights that are both timely and holistic.

Aggregate risk information across levels and functions. This inclusive view helps drive informed decision-making and timely actions to ultimately circumvent or mitigate risks.

[3] "2025 Cyber Considerations," KPMG, 2025

THROUGH THE TPRM LENS

TPRM: A critical factor in resiliency

TPRM plays a critical role in helping to identify critical third parties that could impact a company's ability to remain resilient. Companies should look to align/integrate their TPRM programs with their ERM and operational resilience programs as closely as possible. This involves continuously monitoring third-party performance and risks, implementing, and maintaining controls aligned with the firm's risk appetite. Leveraging tools, technology, and automation can help with efficiently managing and monitoring third parties performance and impact to the company's resiliency.

> **Risk and resilience go hand in hand. The combined effect of volatility, geopolitics, and acceleration in AI adoption continuously changes the attack surface of an organization. By having an integrated approach, organizations can take advantage of the investments in risk management to enhance their resilience capabilities, and vice versa."**

Prasanna Govindankutty
Principal, Cyber Security and Technology Risk
KPMG LLP

How KPMG can help

KPMG helps organizations find the right balance between risk and resilience management. Our approach is integrated by design to bring stakeholder groups together to set the organization's north star, and drive towards outcomes that enable you to take thoughtful risks that drive growth. Our multi-disciplinary teams come with deep experience in enterprise risk, cybersecurity, regulatory compliance, resilience, data, AI, and systems implementation skills.

Our approach is tailored to your evolving business needs, making risk management adaptable and responsive. With our robust network of alliances, tech-enabled solutions, and data-driven methodologies, we provide insights that not only protect your organization but also uncover new opportunities for resilience, growth and stakeholder trust.

Let us help you turn uncertainties into pathways for resilience and value creation.

About the research

Survey Methodology

- **A 15-minute, online survey** among **C-Suite leaders** in the US and was fielded in November 2024.
- The sample includes **208 leaders from public (n=137) and private (n=71) organizations** meeting the following criteria:

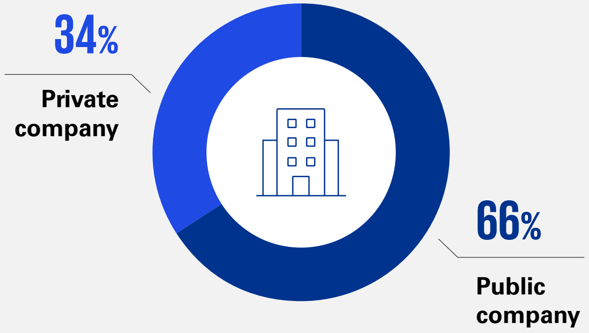
C-Suite job titles including **Chief Risk Officer, Chief Technology Officer, and Chief Financial Officer**

Large enterprise with **at least 1,000 employees**

47% were from companies > $250B. Participants were at least $4B in revenue or $25B in company assets for financial services

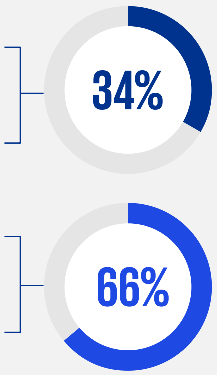
Organizations from a mix of industries

Company type



Company size

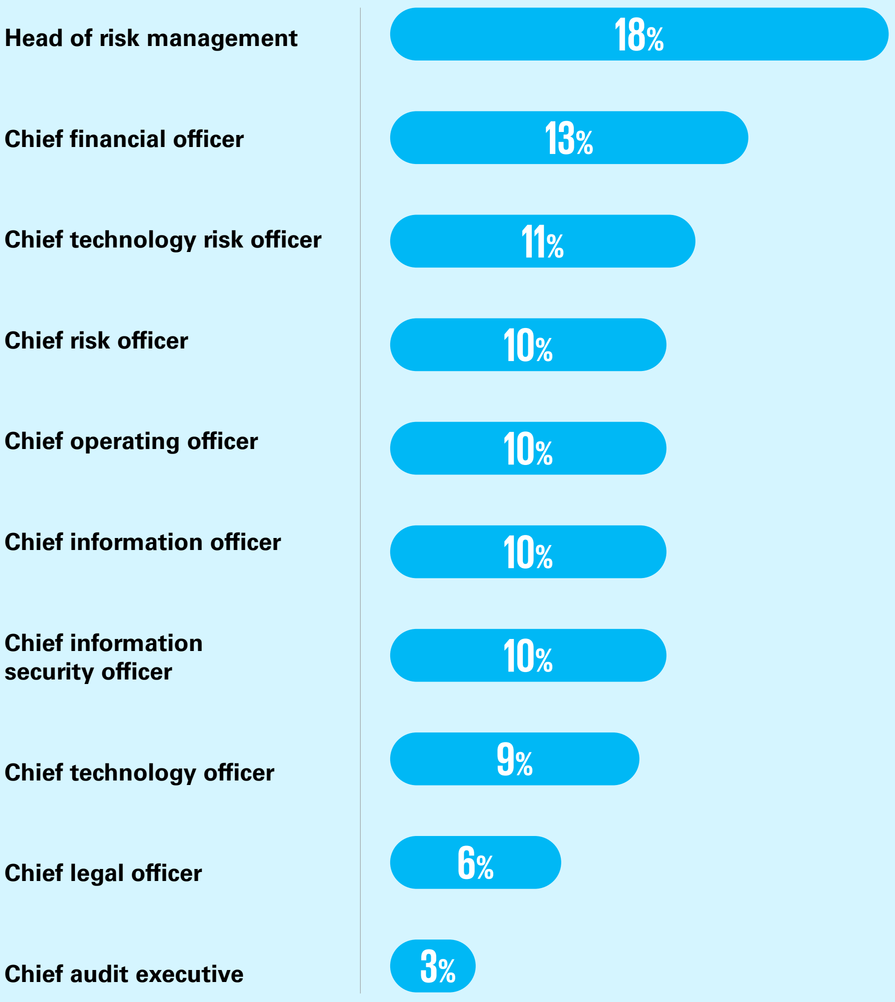
1,000–4,999	4%
5,000–9,999	30%
10,000–19,999	45%
20,000+	21%



Industry

Financial Services	14%	Consumer & Retail	12%
Energy, Natural Resources & Chemicals	14%	Industrial	12%
Healthcare & Life Sciences	13%	Telecommunications & Media	11%
Technology	13%	Fintech	11%

Job title

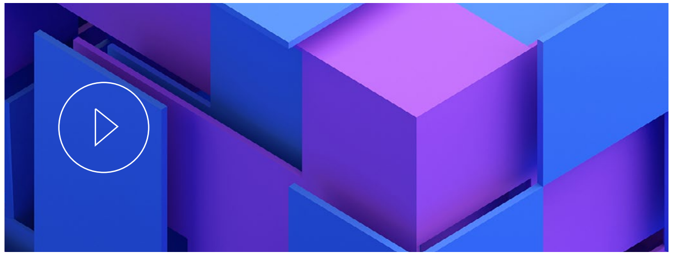


Risk areas overseen

Technology risk	50%
Financial risk	46%
Operational risk	46%
Strategic risk	45%
Cybersecurity risk	37%
Data privacy risk	30%
Legal and regulatory compliance risk	27%
Product and service quality risk	26%
Third party risk	24%
Reputational damage	21%
Business continuity and disaster recovery	21%
Environmental risk	15%
Health and safety risk	13%
Procurement and supply chain risk	12%
Talent acquisition and retention risk	10%
Geopolitical risk	8%

Other relevant resources

Future of Risk



Make operational resilience your North Star

Be organizationally and operationally resilient when—and where—it matters

Cybersecurity considerations 2025

KPMG Chief Risk Officer Survey

Risk readiness depends on risk intelligence

Risk Modernization article series

Building resilience in a hyperconnected world

Subscribe to Risk Factors to receive the latest insights on risk management and resilience.

Contact Information

Joey Gyengo
Principal, Advisory
US Enterprise Risk
Management Leader
KPMG US
E: jgyengo@kpmg.com

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

David Woodson
Director, Advisory
Technology Strategy
KPMG US
E: dwoodson@kpmg.com

Prasanna Govindankutty
Principal, Advisory
Cyber Security Services & Technology Risk Services
KPMG US
E: pkgovindankutty@kpmg.com

Samantha Gloede
Managing Director, Advisory
Global and US Trusted Enterprise Leader
KPMG US
E: sgloede@kpmg.com

The authors would like to thank special contributor, Joy St John.

Learn about us: | **kpmg.com**

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation. KPMG LLP does not provide legal services.

The information contained herein is not intended to be “written advice concerning one or more Federal tax matters” subject to the requirements of section 10.37(a)

(2) of Treasury Department Circular 230.