



Chief Risk Officer Survey

Industry perspective:
**Technology, Media, and
Telecommunications**

read.kpmg.us/CROSurvey



Introduction

The pressure is on for companies to align their risk strategies to their growth strategies and enhance overall trust and resilience. Doing so requires a robust risk function that utilizes the latest and greatest technologies to proactively manage and respond to various evolving risks. Moreover, businesses need a diverse skill set of competent team members who excel at critical thinking.

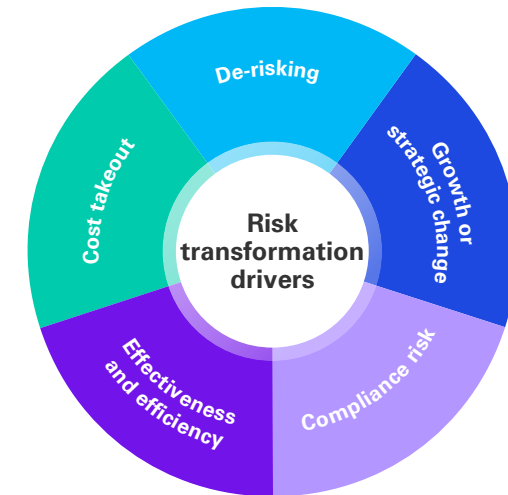
To better understand the specific issues facing corporations, KPMG conducted the 2023 Chief Risk Officer Survey. U.S. respondents included organizations across six industries with at least \$4 billion in annual sales or \$25 billion in assets under management. A survey report was recently released sharing feedback from these risk executives regarding their points of view about the current state of enterprise risk management, as well as their outlooks for the future of enterprise risk functions.

Taking a deep dive into survey responses, this report highlights key takeaways from chief risk officers (CROs) at 41 U.S.-based technology, media, and telecommunications (TMT) firms regarding their top priorities, challenges, and intentions. Their responses, presented with comparisons to other industries, indicate which areas of risk these leaders perceive are most vital to improving risk management practices across TMT businesses.

We found that TMT risk leaders are most challenged by cybersecurity threats and data breaches, complex regulatory changes and compliance obstacles, and the desire to continue digitization across the enterprise to enhance their function's overall efficiency and effectiveness. Dealing with ongoing financial constraints is also a major concern. To work through their top issues, risk executives in TMT tell us they have their sights set on driving optimization through better use of high-powered, integrated risk management systems as well as other modern tools, such as artificial intelligence (AI), machine learning (ML), and predictive modeling. This will allow them to get ahead—and stay ahead—of various compliance regulations. CROs in TMT also indicate they intend to focus on policy management, controls, and employee accountability, as well as increase training for employees, and perhaps consider outsourcing or cosourcing certain tasks.

In this report, we also provide actionable recommendations TMT corporations can use to strengthen their risk management practices, both within their functions and across their organizations. This guidance is aligned to key data insights from our survey, as they pertain to five intersecting drivers of risk transformation (Exhibit 1).

Exhibit 1. Five intersecting drivers



De-risking: Organizations' efforts to reduce risk exposure and hedge against expected market conditions

Growth or strategic change: Organizations' organic or inorganic growth; change in products, services, delivery channels; and/or other large-scale strategic initiatives

Compliance risk: New or emerging regulatory requirements, non-compliance with existing requirements, or need to enhance the relationship with oversight authorities

Effectiveness and efficiency: Increase the quality, consistency, extensibility, and confidence in risk management requirements and outputs

Cost takeout: Reduce the overall costs associated with the governance, maintenance, oversight, and execution of risk requirements and practices



De-risking

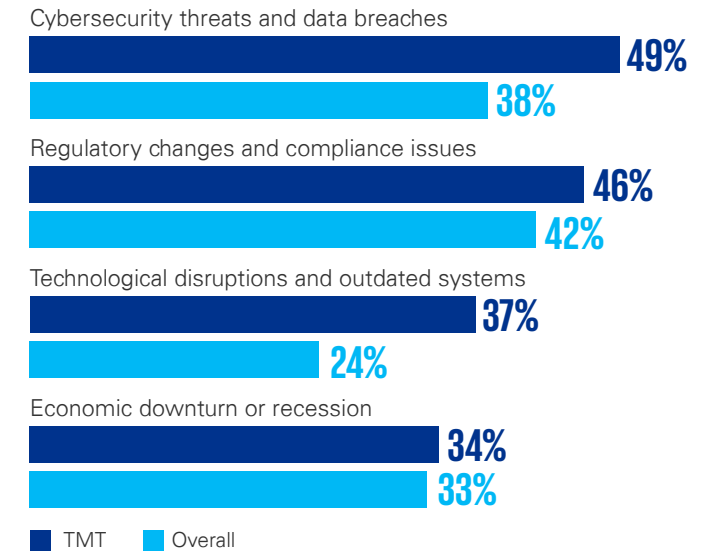
Organizations' efforts to reduce risk exposure and hedge against expected market conditions

Key findings

- In an effort to develop a robust de-risking strategy that prepares risk functions to tackle their biggest concerns in the near future, CROs say cyber threats and data breaches (49 percent) are the top challenges TMT will face over the next two to five years. In our survey, this is the only industry to choose this area as their topmost challenge. This is a result of new and evolving compliance regulations that vary from country to country around cybersecurity protections and data privacy, and often result in product delays for many TMT firms. This could indicate TMT risk teams recognize more than most other sectors the potentially catastrophic damage that a breach or government sanctions for noncompliance (e.g., countries blocking market access) could inflict, spanning beyond even just the company itself.
- To help avoid enterprise risk related to cybersecurity compliance, increasing controls can make all the difference in optimizing a strong risk-minded corporation. In fact, CROs in TMT say the top three areas they will focus on addressing are: improving data and analytics (59 percent); diligence in policy management, controls, and employee accountability (54 percent); and increasing training for employees (49 percent). Notably, TMT is the sector with the largest share of CROs who will improve data and analytics as the primary de-risking method to take on these challenges.

Exhibit 2. Top challenges your organization will face within the next 2–5 years

Q. What do you think are the biggest challenges your organization will face within the next 2–5 years?



Recommendations

- As it relates to cybersecurity threats, a CRO's organization should look to quantify the impact of these threats through cyber risk qualification exercises for their key products and services. This includes the use of both in-house and on-demand external cybersecurity expertise.
- Due to new (and sometimes conflicting) compliance regulations worldwide, TMT products are often held up or delayed in certain regions. To circumvent these types of delays, businesses need a proactive risk management strategy. Doing so means integrating technologies to embed risk information closer to where risk is managed to help save time in meeting compliance goals in the long run.
- Many countries have complex regulations around protecting their citizens' data privacy. A robust incident response plan is essential to preparing for advanced cyber threats and potential data breaches. In fact, technology firms should have privacy assessments built into their product launches.
- TMT companies should look at ways to improve governance and increase controls in an effort to reduce risk throughout their businesses, such as enhanced risk management policies that help every employee think about de-risking opportunities in their daily roles, as well as advanced data analytics and cybersecurity tools, risk-friendly work streams, and ongoing risk management trainings.



“Data sovereignty has become a bigger issue for compliance—and that trickles down to product and security, underscoring how important incident response functions are to quickly deal with issues.”

— Michael Isensee, Partner, Advisory –
Technology, Media, and Telecommunications
Line of Business Leader, Risk Services



Growth or strategic change

Organizations' organic or inorganic growth; change in products, services, delivery channels; and other large-scale strategic initiatives

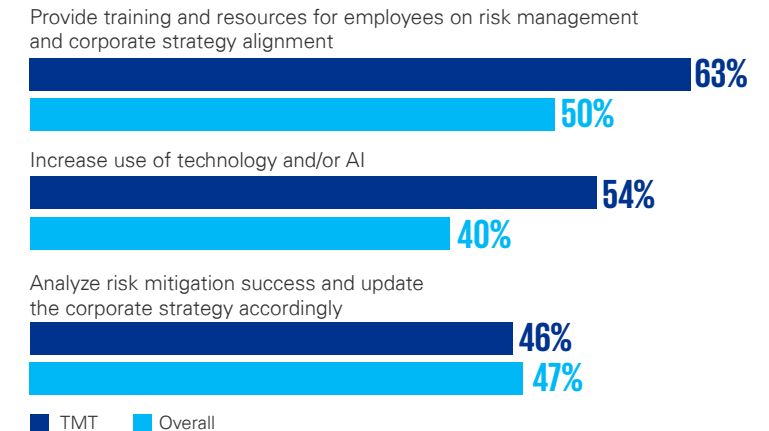


Key findings

- More and more, organizations are looking to align their risk objectives and company-wide growth strategies to ensure their organizations are focused on the right risks at the right time to help drive organizational value. Comparing each sector, TMT has the highest number of CROs who claim providing training and resources for employees on risk management and corporate strategy (63 percent) as a key factor in achieving this alignment goal.
- Harmony between risk management strategy and business growth requires significant buy-in from the top down for risk teams. Luckily, most TMT organizations (83 percent) are well or very well supported by their C-suites. Establishing and maintaining trust and confidence in risk management practices among internal and external stakeholders (44 percent) is driving many TMT companies to transform their risk management execution.


Exhibit 3. Strategies to align risk and strategic goals of the business

Q. Looking ahead over the next 2–5 years, what can your organization do to effectively align or continue to align risk objectives to the strategic goals and priorities of the business?



Recommendations

- Investing in highly capable and business-savvy talent can help risk functions challenge businesses when needed and contribute considerable value. Even the most skilled risk professionals need continued training, particularly around strategic thinking, so they can deliver beneficial insights that align to overall company objectives. They can also identify better ways to bring risk management into areas that have been operating in silos.
- To avoid mistakes and major product delays, training should be available for employees outside of risk departments who deal with risk and compliance. For example, product owners are tasked with updating products when they are held up in regulatory reviews. Educating them around risk can make all the difference in how efficiently a product goes to market in multiple regions. At the same time, educating risk teams to better understand business goals and challenges is also beneficial so that they can help identify better ways to support business growth by enabling an aligned risk and business strategy.



“Like CROs, tech CEOs are concerned about how geopolitics and political uncertainty, emerging or disruptive technology, and cybersecurity concerns may risk the growth of their businesses, highlighting the need for proactive strategies to address these matters.”

— Mark Gibson, Global Head of Technology, Media, and Telecommunications, KPMG International

Compliance risk

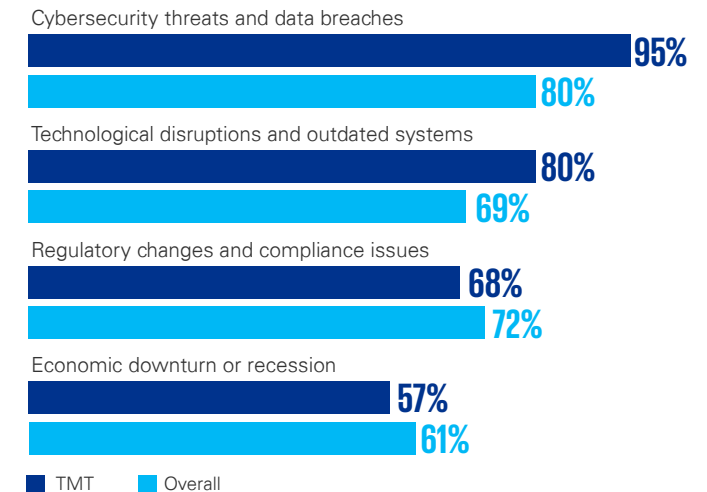
New or emerging regulatory requirements, noncompliance with existing requirements, or need to enhance the relationship with oversight authorities

Key findings

- While CROs in TMT listed regulatory changes and compliance issues as the second-biggest challenge facing their organizations over the next two to five years, 68 percent say they are well or very well prepared to respond to and appropriately manage this risk, which is slightly less than the readiness level specified by most other industries (72 percent). An overwhelming majority (95 percent) of TMT risk leaders feel they are well or very well prepared to tackle cybersecurity threats and data breaches, which also has a major regulatory component to it.
- Now more than ever, the TMT sector faces new roadblocks in the forms of varying regulatory changes and increased compliance requirements worldwide that require substantial budgets and other resources to confront. Notably, nearly all CROs (90 percent) in TMT plan on increasing their budgets within the next 12 months. Most TMT risk leaders allocated funds to support compliance monitoring and regulatory reporting over the past year (95 percent) and plan to continue to invest in this area over the next 12 months (85 percent), signaling they expect regulatory pressures to persist.

Exhibit 4. Preparedness to address risk challenges

Q. Of the top challenges your organization will face within the next 2–5 years that you selected, how prepared is your organization to respond to and appropriately manage these risks?



Percentages represent respondents who answered “Well prepared” or “Very well prepared.”



01

02

03

04

05

06

07

08

Recommendations

- From the start, prepare to make changes to adhere to a variety of different and conflicting regulatory requirements, beyond just data privacy and cybersecurity. Certain regulations, such as the EU Digital Services Act, Digital Markets Act, and AI Act have expanded their focus from cybersecurity protections to become much broader. As a result, the integration of these compliance efforts is of critical importance to achieve successful outcomes at manageable levels of effort. This includes reinforcing compliance considerations during regular business process activities and prior to product launches, such as privacy assessments, as an important practice.
- Prioritize compliance risk as an integral part of business priorities. Expand efforts to understand the principles that regulators are looking to see, and appropriately assess all potential risk impacts.
- Align data and cybersecurity budgets with the need for compiling and sharing internal data in light of new tax and statutory compliance requirements. Rapid globalization, new developments in tax laws, changes in accounting standards, and increased demands from tax authorities are all increasing the burden on tax and finance departments. In an industry that relies on new ideas and paves the way for new modernization techniques, TMT corporations must figure out how to meet compliance obligations without stifling innovation. Staying ahead of the game when it comes to compliance requires the latest and greatest technologies, such as AI, ML, and automation. Modernizing compliance risk capabilities by building scalable and integrated risk and compliance programs will help risk deliver the same or expanded capabilities, but in a more efficient way. Simplification and harmonization across risk frameworks, technology, reporting, and services are also helpful to the organization as a whole.

“Many TMT companies grapple with new compliance demands and regulatory enforcement, which heightens risk, necessitates continual talent development in risk and compliance, and is driving greater investment in analytics, automation, and other tools.”

— Michael Isensee, Partner, Advisory –
Technology, Media, and Telecommunications
Line of Business Leader, Risk Services



Effectiveness and efficiency

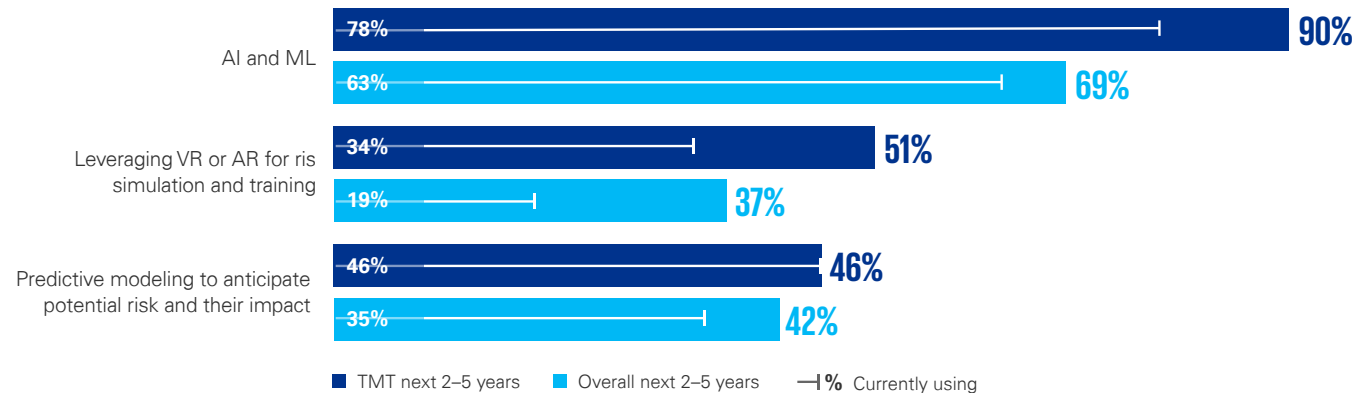
Increase the quality, consistency, extensibility, and confidence in risk management requirements and outputs

Key findings

- For budget allocation, the topmost areas for TMT risk executives spending today is for technology-driven risk management (100 percent) and information technology infrastructure and security (98 percent). Within the next year, these are expected to remain the most-funded areas. Third on their list is operational risk assessments and process improvement (93 percent), which they plan to decrease by 3 percent over the next year. Despite the slight decline in budget for this area, risk leaders clearly see the continued importance of identifying and mitigating operational risks within their organizations. Investing in each of these three areas increases the overall value and efficiency of risk management functions and their value added to every area of an organization.
- TMT has been leaning on digital tools and solutions to accelerate risk management processes to enhance their function's credibility. So far, industry leaders say they have leveraged AI and ML (78 percent), and predictive modeling for anticipation of potential risks and their impact (46 percent). Over the next two to five years, even more TMT risk leaders will rely on AI and ML (90 percent) and virtual reality (VR) or artificial reality (AR) (51 percent). In every area, present and future, TMT exceeds the number of respondents in other sectors enhancing their risk management processes with leading digital tools for optimized efficiency and effectiveness.

Exhibit 5. Tools to optimize risk management

Q. Which digital tools/solutions are you using to accelerate risk management processes within your organization? Looking ahead to the next 2-5 years, which digital tools/solutions do you believe would further assist and optimize your risk management processes?



Recommendations

- Modern technology allows companies to improve, update, and enhance their risk functions so they can improve risk efficiency and effectiveness. A leading digital environment enables the risk function to embed risk management closer to the point of risk origin, automate routine processes, reduce manual efforts, and accelerate access to risk information. Combining the best digital tools across the risk ecosystem is the best way to empower and proactively transform how risks are detected and addressed.
- In an industry that makes its business around inventing and implementing technology, TMT companies have a unique ability to create use cases around their own products from within their risk portfolios, but they must balance efficiency, performance, and innovation to be truly effective.
- As digitization is expanded, organizations must also change to support new tools and practices, including the integration of digital platforms across various functions and teams. This will help sustain efficiency through an integrated, digital-first strategy and operating model, rather than building one-off solutions created in a vacuum.

“CROs need to balance and manage product, security, and regulatory requirements and build a strategy that proactively prioritizes each of these across the organization.”

— Brian Geffert, Principal, Advisory
— Technology, Media, and
Telecommunications Line of Business
Leader, Cyber Security Services



01

02

03

04

05

06

07

08

Cost takeout and optimization

Reduce the overall costs associated with the governance, maintenance, oversight, and execution of risk requirements and practices

Key findings

- Notably, TMT CROs say they would consider outsourcing technology-driven risk management (46 percent) more than any other sector to effectively reduce spending. That is because TMT businesses understand the intricacies of managing these types of risk and the need for specialized expertise to address them effectively.
- Of course, major technology outsourcing comes with a higher risk profile. While there is the potential for significant cost savings, most CROs in TMT are somewhat concerned (46 percent) with third-party/vendor risks due to technology outsourcing or integration, more so than other technology adoption issues.
- Unfortunately, the TMT industry has made news in recent years for mass layoffs at some of the sector's biggest names. Hiring new talent to bolster risk functions is extremely limited, with corporations continuously being asked to do more with less. That is why investment in existing employees, through training and upskilling is favored (44 percent) over hiring more talent (34 percent) when preparing for and addressing challenges.

Exhibit 6. Risk management organizational models

Q. Which areas of risk management within your organization would you consider outsourcing or cosourcing to external partners in order to enhance the efficiency and effectiveness of risk mitigation strategies?



01

02

03

04

05

06

07

08

Recommendations

- Alignment of risk and overall business strategies can help organizations strike a balance between cost savings and optimization. With technology at the heart of risk management, finding a middle ground between implementing the best tools for each risk area and choosing which tasks should be outsourced is vital to an optimized risk function.
- Outsourcing, cosourcing, and on-demand arrangements for key areas (e.g., specialized security skills that are not cost effective to keep in-house) can result in tremendous cost savings. Relying on vendors that specialize in certain complicated areas, such as cybersecurity; environmental, social, and governance; and tax takes the burden off organizations to handle the entire risk ecosystem, all at once, and all on their own.
- Create an ongoing and enterprise-wide risk management strategy that ensures third-party vendors are themselves appropriately managing their risks, including overall security. Since risk associated with third parties can so heavily impact the companies that partner with them, rigorous vetting must be performed to ensure hiring them will be a true cost-saving measure.
- Weigh outsourcing and cosourcing decisions against the process changes and additional resources required to maintain the necessary level of risk control and governance. Risk leaders must find a boundary where organizations can maintain quality without inadvertently creating new third-party risk.

“Technology, media, and telecommunications companies are turning to professional services firms that have core competencies outside their own—for disciplines in domestic and global regulatory compliance and tax, for example—to provide managed service delivery models. This approach allows organizations to focus on their primary business while gaining access to the provider’s scale in both human capital and outsized investments in technology, while proactively managing risk and compliance and driving operational efficiency.”

— Dean Kamahale, Principal, Tax Sector Leader — Technology



01

02

03

04

05

06

07

08

How KPMG can help

KPMG Risk Services brings the strategic vision and technical edge to help you earn the trust of your stakeholders. Our deep TMT industry skills concentrated in risk, regulation, cyber, and ESG, and our time-tested change experience, combine to create one powerful capability.

KPMG teams can help you anticipate and balance risk to generate value and a competitive advantage across your enterprise. By incorporating a detailed approach to risk, compliance, cyber, and ESG, we can help you identify new opportunities.

We are obsessively focused on the delivery of your strategy, your priorities, and your agenda. Using tools and solutions that accelerate your modernization journey and balance risk, we then apply deep domain knowledge across the spectrum of risk and regulatory issues, along with our skills in risk, technology, and consulting, to help drive borderless collaboration to convert the opportunities of risk into a sustainable competitive advantage for your organization.

Learn more: visit.kpmg.us/RiskServices



01

02

03

04

05

06

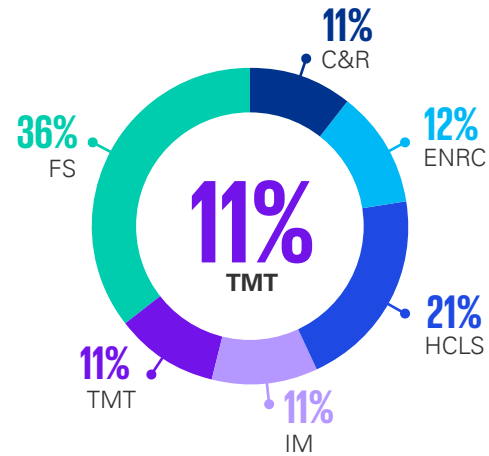
07

08

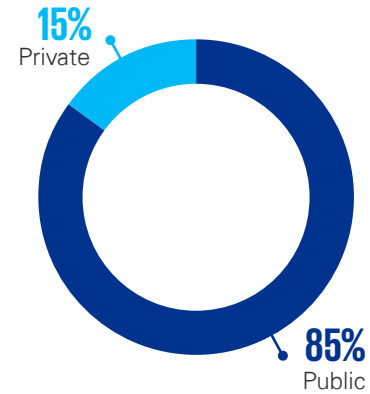
Research methodology

From July to September 2023, KPMG conducted an online survey of 390 enterprise risk officers representing U.S. organizations across six industry sectors with at least \$4 billion in annual sales or \$25 billion in assets under management (AUM). Forty-one respondents participated from the TMT sectors. Our research is designed to track trends in enterprise risk management and provide an outlook on the future of the enterprise risk function. Survey questions explore risk officer views on current and expected trends in the following areas: Risks and readiness, activities and investments, roles and approaches, and maturity and modernization.

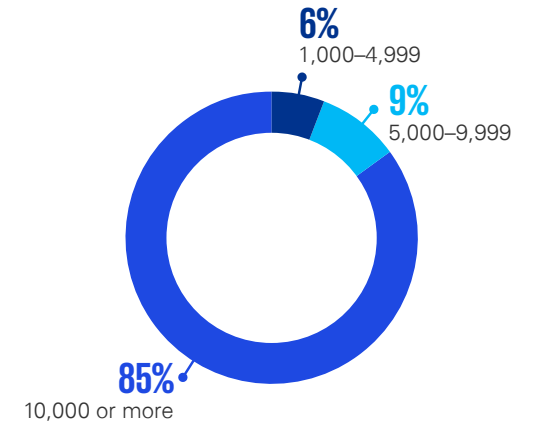
Organizational sector



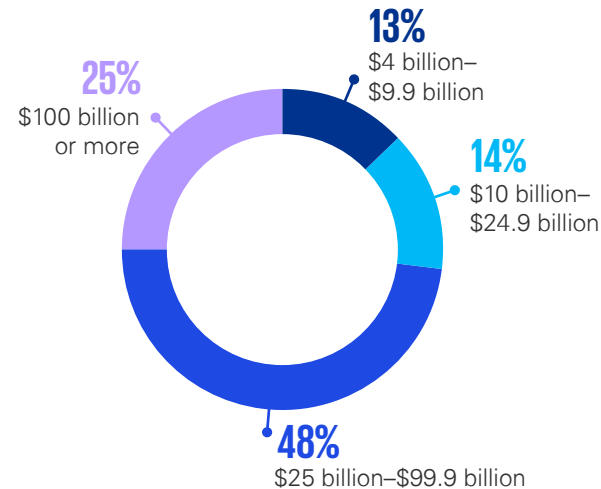
Organization type



Full-time employees in the company (Globally)



Company's annual revenue



Of the 390 enterprise risk officers responding to the survey, 41 respondents (11%) participated from the TMT sectors.

Notes: N=390; Single select; Percentages may not total 100 due to rounding.



Authors



Michael Isensee
*Partner, Advisory – Technology,
Media, and Telecommunications Line
of Business Leader, Risk Services*
misensee@kpmg.com



Mark Gibson
*Global Head of Technology,
Media, and Telecommunications,
KPMG International*
mgibson@kpmg.com



John Kemler
*Principal, Advisory, FS Risk,
Regulatory & Compliance*
jkemler@kpmg.com



Brian Geffert
*Principal, Advisory — Technology, Media,
and Telecommunications Line of Business
Leader, Cyber Security Services*
bgeffert@kpmg.com

KPMG is recognized as a leader in risk consulting



Financial risk



Third party assurance



Client advocacy in risk*

KPMG ranked No. 1 across multiple risk categories in Source's report, *Perceptions of Risk Firms in 2023*.

The Source study, *Perceptions of Risk Firms 2023*, is based on a U.S. client and prospect perception survey about risk consulting firms, led by Source. It reveals what 300 senior users in the U.S. think about the 16 leading risk advisory firms and examines how clients see firms differently as they move from awareness, to shortlisting a firm, to becoming a direct client. The report is intended to help in understanding each firm's positioning in the market and the overall competitive landscape in which they operate. For more information please visit: <https://www.sourceglobalresearch.com/>

*Advocacy score is based on the percentage of KPMG client respondents that say they would use the firm again and would put their personal reputation on the line for the firm.

 [visit.kpmg.us/SourceRankings](https://www.kpmg.us/SourceRankings)



01

02

03

04

05

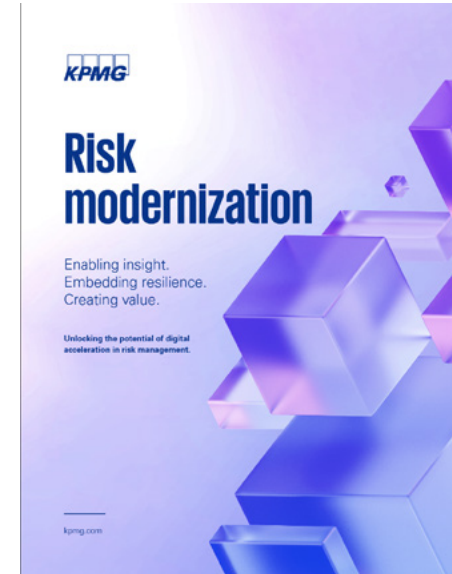
06

07

08

Related thought leadership

Read the full report: read.kpmg.us/CROSurvey



 [Subscribe to receive Risk and Cyber insights](#)

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.

© 2024 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

DASD-2024-14808

Please visit us:



kpmg.com



[Subscribe](#)