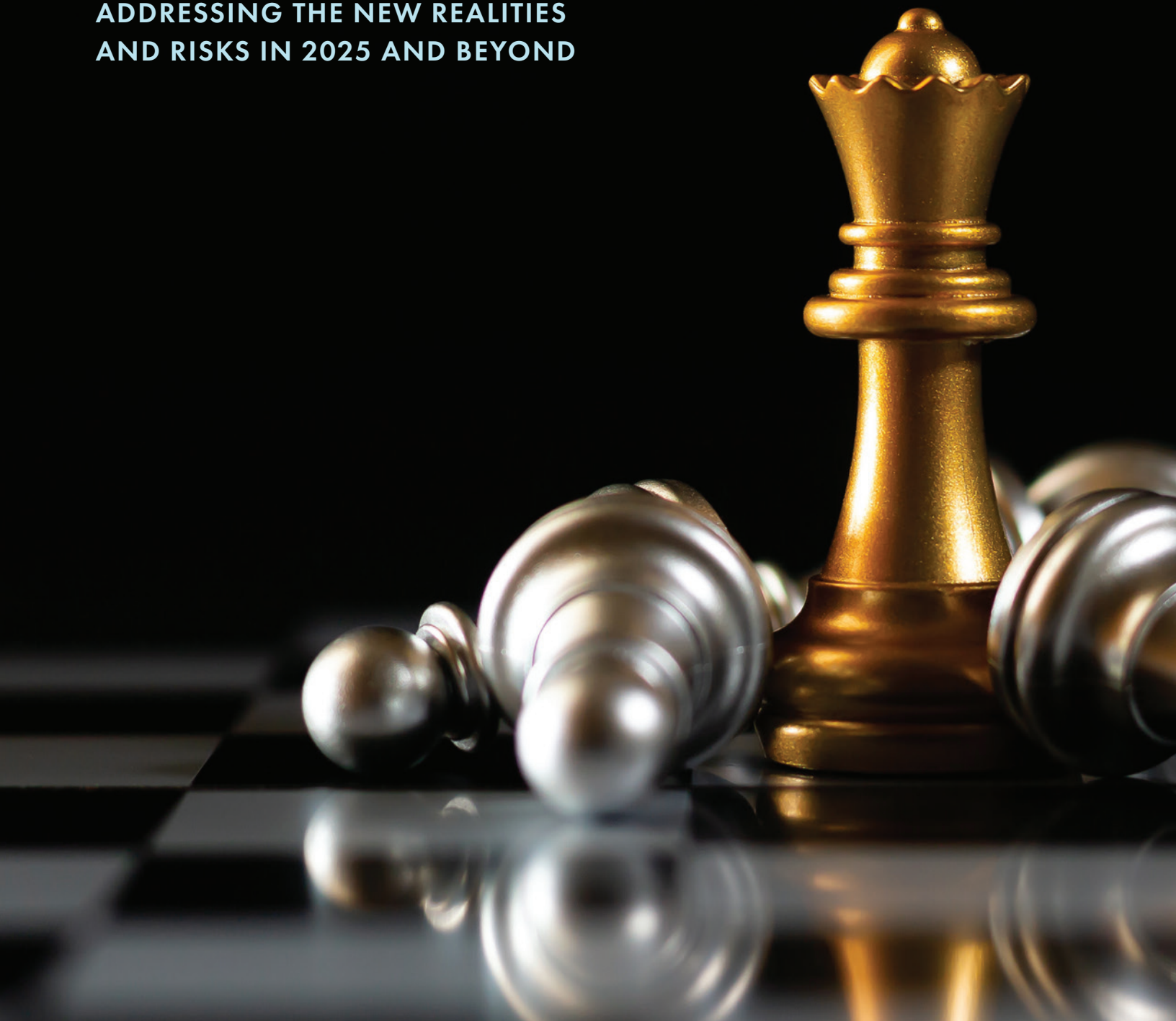
riskonnect

The 2025 New Generation of Risk Report

ADDRESSING THE NEW REALITIES AND RISKS IN 2025 AND BEYOND



Executive Summary

Political uncertainty is climbing. Geopolitical shocks and cyberattacks are still hitting companies hard. Economic uncertainty lingers. And AI is advancing faster than governance can keep up. Agentic AI – the latest wave of AI technology – is already here, yet many companies are still wrapping their heads around generative AI and its risks three years into the technology hitting the mass market.

These forces are creating a high-stakes environment that demands faster, sharper, and more proactive responses. Are risk management strategies evolving quickly enough alongside the landscape?

Riskonnect surveyed more than 200 risk, compliance, and resilience professionals worldwide to uncover today's most pressing threats and to see if organizations are ready for this new generation of risk.

The 2025 New Generation of Risk Report reveals that while leaders are making meaningful progress in important areas, such as worst-case scenario planning, AI adoption, and building plans for geopolitical risk (which were largely absent a year ago), critical gaps remain. The data paints a clear picture that risk management is increasingly viewed as a strategic business function. But it's in a pivotal state of transition, and companies must invest decisively to realize its full potential and strengthen its impact.

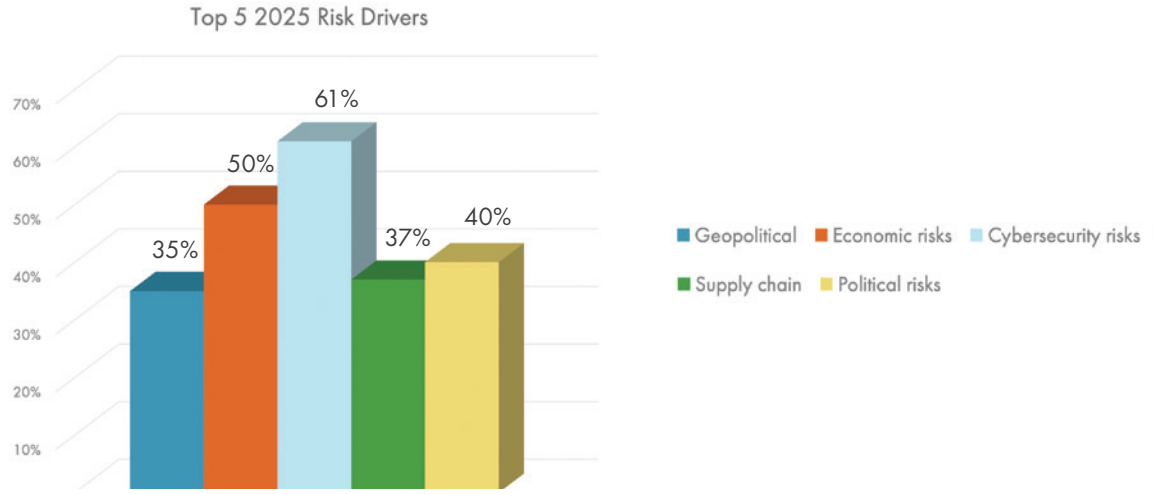
Political Risk Is Rising as a Top Threat

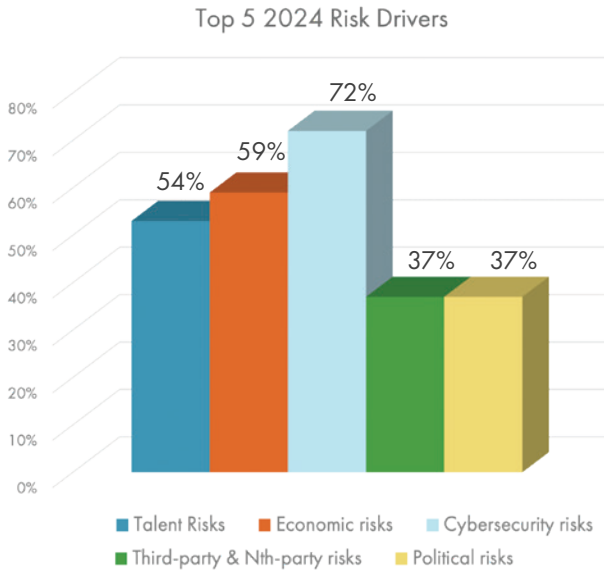
Political risk has climbed into the top-three corporate threats, rising from fifth place last year. Nearly all risk leaders (97%) say political risks are impacting their business in some way, and 40% describe the impact as significant or severe.

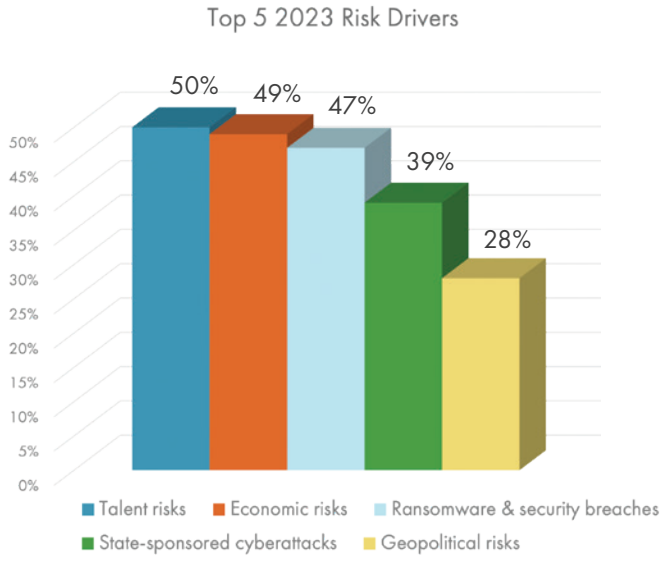
Companies say they have had to stall or slow hiring (37%), delay major tech investments or capital expenditures (28%), and delay expansion plans (23%) because of domestic political instability. Others have had to diversify supply chains and/or reshore operations (27%).

It's not surprising that political risk is a high concern, as these risks can directly affect corporate strategy and stability. Today's climate – especially in the U.S. where tariffs, escalating trade tensions, and various policy and regulatory shifts are heightening uncertainty – is impacting many companies' margins, costs, market access, operations, supply chains, and growth strategies.

What is surprising, however, is that only 17% of respondents say they feel very prepared to assess, manage, and recover from political risks when they had time to prepare. Policy changes were signaled in advance with campaign promises, which indicates that companies either doubted these changes would materialize and didn't take steps to get ready, or they underestimated the scale and speed of the shifts and the impact.







This serves as a wake-up call. Companies often struggle to act on known risks that feel distant – or they underestimate the scale of an event. Consider the COVID-19 pandemic. Some risk leaders recognized the potential threat of a pandemic on their risk registers, but almost none prepared for the sheer scale of the impact from the shutdowns.

Resilience depends on moving from recognition of risks to preparing for them before disruption hits.

Companies Are Waking Up to Geopolitical Risk

While preparedness for domestic political risk lags, the picture looks different when it comes to geopolitical threats.

Geopolitical risk planning is gaining ground: Two-thirds (66%) of companies entered 2025 with a plan for managing geopolitical volatility – a considerable jump from the 19% that said they had a plan last year.

Bracing for a Slowdown:

Nearly seven in ten (69%) risk leaders expect an economic downturn in the next 12 months. Of those, 66% believe it will be mild or short-lived.

But reality hit harder than forecasted. Of those that had a plan for these types of events, 30% said the impact was worse than expected. Of the roughly one third that did not have a plan, 26% reported a bigger-than-expected disruption. This is a proof point of how fast the risk environment is evolving and a reminder that risk events rarely unfold as imagined. This is especially true for geopolitical risk events that are inherently volatile and difficult to predict with complete accuracy.

"The fact that more companies are planning for geopolitical risk should be celebrated. The purpose of planning is to prepare for events that are far more extreme than anticipated. The act of planning builds resilience and increases an organization's ability to adapt and respond with speed and accuracy when an event hits. Those who have a plan are in a much better position than those who don't," said Jim Wetekamp, Riskonnect CEO.

Despite the increase in planning, only 18% of risk leaders say they are very prepared to assess, manage, and recover from geopolitical risks. Most organizations still focus their planning on known threats like trade policies and specific conflicts instead of on cascading effects such as supply choke points, cyberattacks, and instability in secondary regions.

Volatility and disruption are the norm today, not the exception. Yet, preparedness for unpredictable risk events remains strikingly low. Only 9% of leaders in 2025 feel very prepared to assess manage, and recover from a future unknown and unpredictable risk event, up only slightly from 4% in 2024 and 5% in 2023.

Even risks that are well known and predictable can spiral in unforeseen ways – through their speed, scale, or the ripple effects they create. In both cases, the takeaway is the same: It pays to prepare.

Trade Wars Could Trigger an Influx of Cyberattacks

Geopolitical volatility creates conditions ripe for cyberattacks. In fact, 62% of risk leaders say if the U.S. adopts more restrictive trade policies or engages in open conflict with other nations on a long-term basis, the biggest risk to their organization is increased cyber exposure from state-sponsored attacks and reduced federal cyber investments.

Nation-state actors typically target companies to steal intellectual property or sensitive data for political or economic gain. When trade frictions escalate, hostile actors have greater incentives to attack. Many of these attacks infiltrate through digital vulnerabilities at third parties. The reduced cybersecurity oversight at the federal level puts more ownership on companies to strengthen their defenses.

Other serious ripple effects of a prolonged restrictive trade environment include higher production and indirect costs (48%), severe supply chain disruptions and shortages (47%), and higher domestic labor costs (31%).

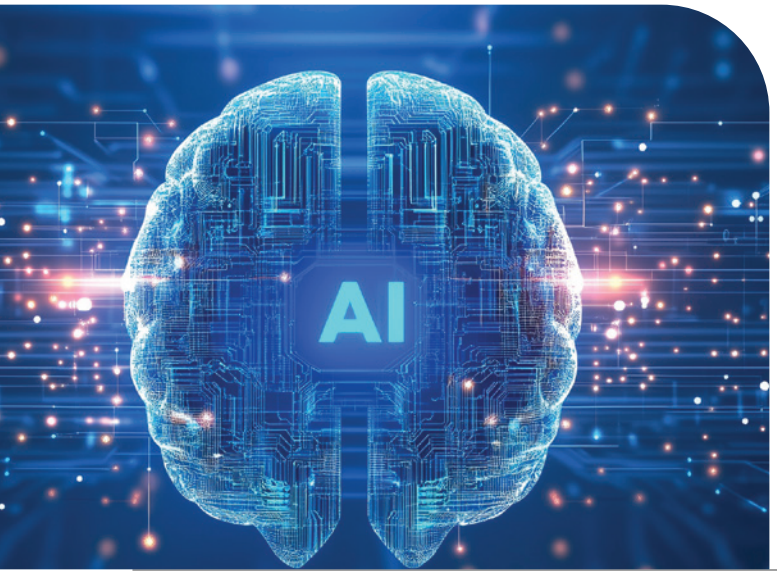
Agentic AI Is Entering the Risk Landscape

Companies are seemingly flying blind on one of today's most impactful – yet risky – technologies. Nearly 60% of risk leaders say their companies are considering incorporating agentic AI solutions into their operations or products. Yet over half of those leaders (55%) haven't assessed the risks.

Perhaps even more concerning, a noteworthy share (15%) of risk leaders say they don't know whether their organization is considering incorporating agentic AI into its operations or products – which is a risk in and of itself.

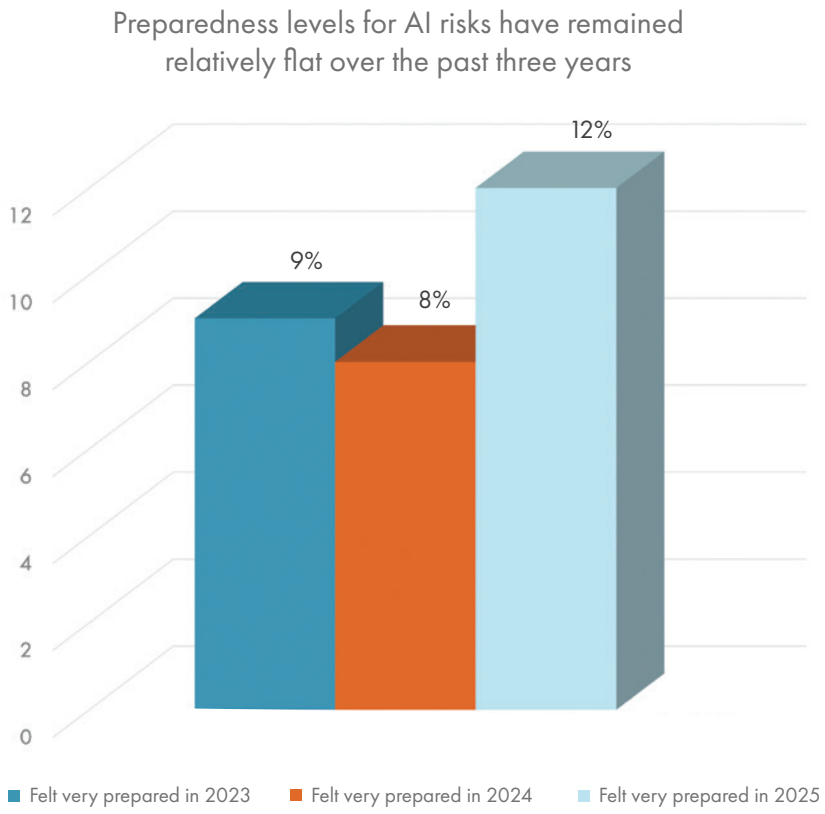
This lack of risk management and oversight over agentic AI is dangerous. AI needs to be treated like any other enterprise risk and built into risk management frameworks, governed proactively, and managed with the same rigor as cybersecurity, compliance, and other risk domains. Right now, most companies aren't set up to adapt to how quickly AI is evolving – and the risks are too big to ignore.

Risk leaders say the biggest risks they foresee from deploying agentic AI are data privacy and security issues (68%), autonomous decisions that conflict with business goals, legal requirements and/or long-term strategy (52%), and unintended actions from runaway processes (38%), such as unauthorized transactions, incorrect pricing changes, or installing the wrong software update.



> ***"Agentic AI is a new and critical category of enterprise risk. The autonomous execution of tasks is bound to bring tremendous efficiency gains, but also the potential for runaway processes or cascading failures if not managed properly. Companies need accountability and continuous oversight designed for autonomous, adaptive systems. Start building it now. Manage AI risk just as you would for any other major risk under your roof."***
>
> - Jim Wetekamp

Glaring Gaps Remain in Generative AI Risk Management



Only 12% of companies today say they feel very prepared to assess, manage, and recover from AI and AI governance risks.

That's troubling as many organizations are actively testing and adopting generative AI tools. And shadow AI use is prevalent, with a recent study finding workers at more than 90% of companies using personal chatbot accounts for daily tasks, often without approval from IT.[1]

The lack of preparedness and confidence is likely low because companies are still overlooking critical areas when it comes to AI oversight:

- **42%** of companies don't have a policy in place to govern the use of AI by employees.
- **72%** don't have one for the use of genAI by partners and suppliers.
- **75%** say they don't have a dedicated plan to specifically address genAI risks, including deepfakes and AI-driven fraud attacks.
- **15%** say they have a budget specifically directed at mitigating AI-related risks, which is about the same percentage as last year.
- **23%** have a policy against using foreign AI models such as Deepseek.

Training on AI risks is trending in the right direction. Some 32% of companies say they have formally trained or briefed the entire company on risks related to genAI, up from 19% in 2024 and 17% in 2023. While training is essential, it can't solve for everything, and companies need to complement training with clear policies and controls.

Surprisingly, about a quarter of companies still aren't taking any meaningful action on generative AI risks: 26% of respondents report having no policies, formal training, budgets, or dedicated plans to address AI risks.

[1]Fortune, "The 'shadow AI economy' is booming: Workers at 90% of companies say they use chatbots, but most of them are hiding it from IT"

Critical Third-Party Exposures Persist

Companies remain dangerously vulnerable to third-party and nth-party risks – yet many risk leaders underestimate the exposure. Most (85%) say they have a business continuity and resilience plan in place to keep their organization running in the event of a major IT outage or cyber incident at one of their business-critical service providers. But upon a deeper look, the data shows a fundamental weakness: Their ability to assess and monitor supplier risks stops at their immediate suppliers, leaving hidden vulnerabilities buried deeper in the digital supply chain.

The proof is in the numbers:

- **45%** of risk leaders say they can only assess and monitor their tier 1 tech partners.
- **8%** say they can assess and monitor their tier 1 partners, their suppliers, and their suppliers' suppliers.
- **16%** admit they can't monitor and assess the risks of their critical third-party tech partners at all.

That last number is especially concerning, particularly for large enterprises. Every company needs to at least be able to assess and monitor their immediate tier 1 partners. In an environment where hackers often exploit third parties, this lack of visibility isn't just risky, it's reckless.

The overall lack of visibility persists even though 66% of risk leaders say they've reviewed and made updates to their IT and cyber risk management strategy in light of major recent disruptions such as the Crowdstrike outage or MOVEit breach. This indicates companies are overlooking critical third-party vulnerabilities.

While companies might have business continuity and resilience plans on paper, in practice they are relying on an incomplete picture and assumptions about third-party reliability. Without the capacity to assess and monitor suppliers' suppliers, organizations are vulnerable to disruptions throughout their extended supply chain. This lack of visibility can also inhibit response and recovery efforts when incidents occur.

30% say third-party and nth-party risks aren't having an impact or are just having a minimal impact on their business – evidence that many still underestimate the danger.

Risk Teams Are Leaning into AI to Keep Up

AI adoption in risk management is growing. In 2024, 62% of companies were using or planned to use AI to help manage risk. By 2025, that figure has jumped to 70%.

Top ways risk leaders are leveraging AI include:

- **34%** Assessing risks
- **28%** Risk forecasting
- **28%** Scenario planning and simulations
- **28%** Creating risk registers
- **28%** Surfacing risks that they hadn't previously considered

The Hidden Danger of Shadow AI

34% of VP and C-level risk executives say they are not considering incorporating agentic AI into their operations or products, compared to only 20% of directors, managers, and below. This disconnect signals a growing threat: shadow AI, where employees adopt tools outside official channels, creating blind spots and unmanaged risks.

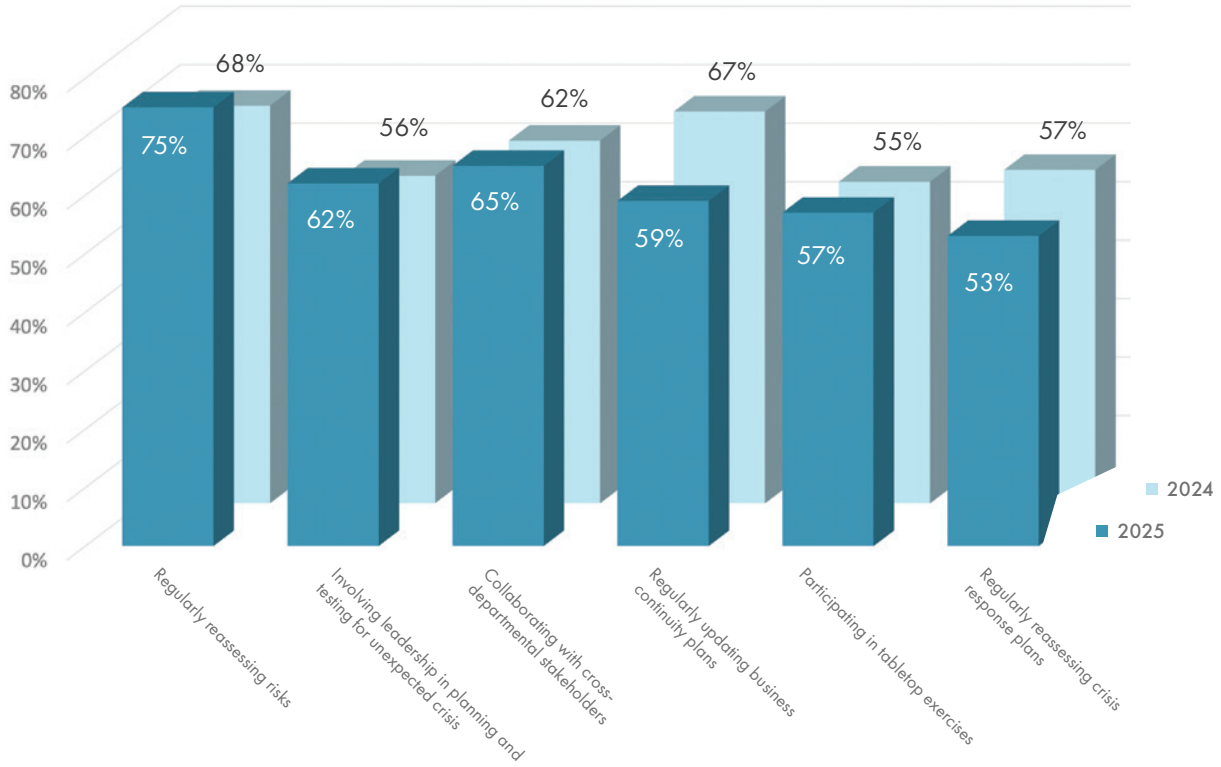
Assessing risks jumped to the #1 use case for AI in risk management, moving from 29% in 2024 to 34% in 2025.

One of the biggest areas in which AI adds value and helps elevate the strategic impact of the risk function is with scenario planning – an exercise that has become essential in today's fast-moving risk environment. Scenario planning gives companies a structured way to play out multiple plausible scenarios, test their strategies against different conditions, and identify vulnerabilities before disaster strikes. It helps leaders reduce risk, build resilience, make more informed decisions, and remain agile in the face of many types of events.

AI makes simulations faster, smarter, and more realistic, and it can fill in critical information gaps. Traditional approaches often rely on historical data and human judgment, which can miss signals and fail to capture the speed of today's disruptions. AI synthesizes vast, diverse data sources, from economic indicators to supply chain flows and regulatory developments, as well as current events such as shifts in trade policy and tariffs, to produce a more complete picture. Risk leaders using AI can rapidly model multiple complex scenarios without personal bias, understand a wider range of plausible scenarios, and get actionable insights to prepare for risk events.

Sixty-one percent of risk leaders say they've simulated their worst-case scenario, which is up significantly from 44% in 2024 and 37% in 2023. That's encouraging progress and could be attributed in part to greater AI adoption. Thirty-nine percent of companies still aren't conducting this critical exercise, which shows it needs to be taken more seriously.

Other steps teams take to plan for crisis scenarios

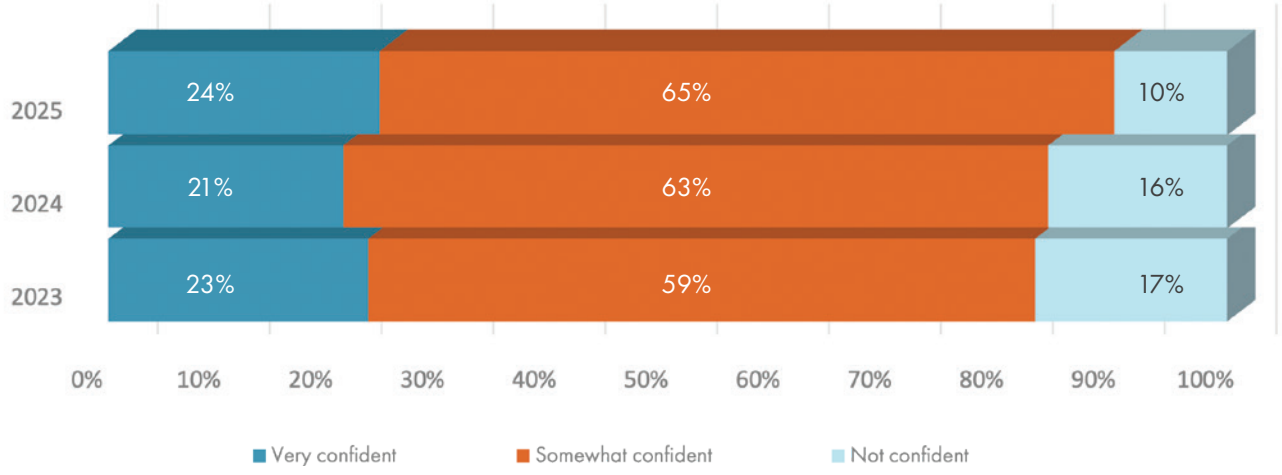


Confidence in Risk Data Is Growing

Risk management is finally moving out of spreadsheets. Last year, over half (53%) of companies said they mostly or only use spreadsheets to manage risk. In 2025, that number dropped to 40%, while 60% now say they mostly or only use software to manage risk.

The shift matters. As companies lean into software, confidence in risk management data is simultaneously improving. Only 10% of leaders say they aren't confident in their data/it can't be trusted, which is down from 16% who said so last year. That six-point drop marks real progress after years of stagnation and shows that investments in software are paying off

Confidence in the Accuracy, Quality, and Actionability of Risk Management Data YoY



Risk Is in the Spotlight, But Budgets Are at a Standstill

Risk representation in the C-suite is growing. Sixty percent of companies now have a chief risk officer, compared to 52% over the past two years. The growing presence of CROs and risk expertise at the C-level signals that organizations increasingly recognize risk management as a priority and that risk leaders are critical enablers of the company's strategy and growth.

Despite this heightened visibility and influence, budget growth for the function has remained relatively flat at a time when the risk environment is evolving at unprecedented speed. Only 28% of risk leaders report an increase in technology budgets, a figure that has stayed the same over the past three years. Nearly two-thirds say budgets haven't changed at all.

Risk leaders are being asked to address more complex threats, provide greater strategic input, and build resilience across the enterprise – all without a corresponding meaningful increase in resources. The pressure is on risk teams to do more with less, which makes tools like AI and automation even more essential to providing strategic value and meeting expectations at the board and executive level.

Elevate Your Risk Function

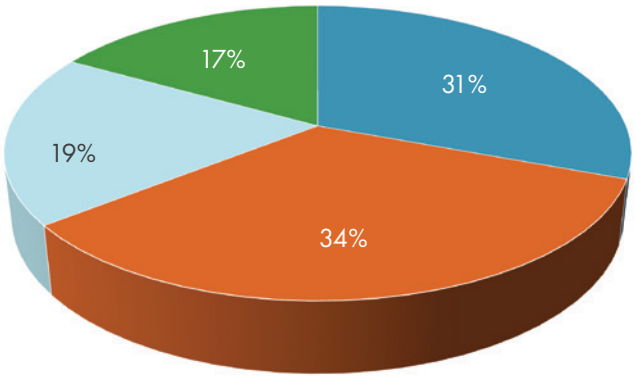
Risk leaders don't just need to keep up with this new generation of risk. They need to get ahead. A few steps to take now:

- **Embrace AI with governance.**
  AI isn't a side project. Treat it as a core enterprise risk and manage it under the same roof as any other risk.
- **Scenario plan.**
  Don't wait for risks to materialize. Stress-test your playbook with AI-powered simulations that consider shocks and risk factors you might otherwise discount.
- **Look past your tier 1s.**
  Hone your ability to assess and monitor risks across your entire digital supply chain, especially as third parties are often the front door for bad actors. Even if you can't get granular on every layer, be ready to manage the fallout.
- **Elevate your impact with AI.**
  Strategically leverage the technology in key areas that save you time and enable you to be more proactive and focus on what matters.
- **Invest in technology.**
  This is key for staying ahead and managing the full spectrum of risk.

This new generation of risk is not just defined by the sheer scale and speed of emerging threats, but also by the ways in which companies are preparing to meet them. Are the steps you are taking bold enough, fast enough, and strategic enough to stay ahead?

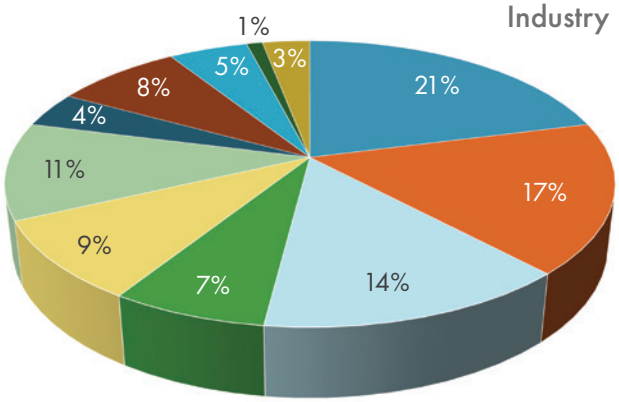
Demograhics of the 226 risk and compliance professionals who responded to the survey.

Role



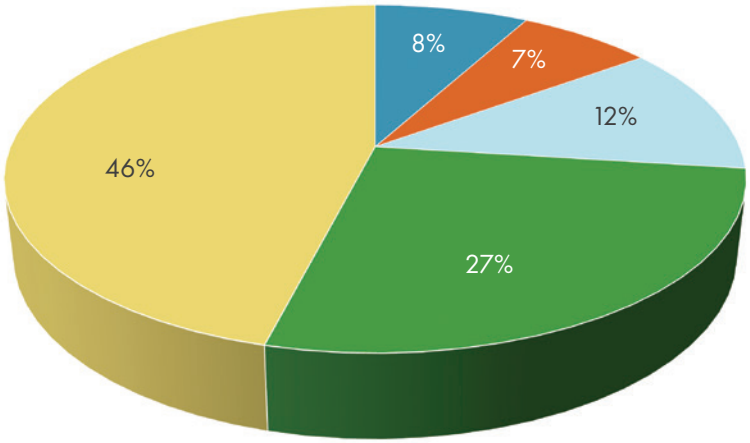
- Director in risk, compliance, or resilience
- Manager in risk, compliance, or resilience
- Analyst, specialist, or coordinator in risk, compliance, or resilience
- VP or C-level risk, compliance, or resilience executive

Industry



- Financial Services
- Public Sector
- Healthcare
- Insurer and TPAs
- Energy
- Transportation
- Infastructure
- Retail
- Manufacturing
- Insurance Brokers
- Aerospace & Defense

Company Size



- Under 250 employees
- 251 – 500 employees
- 501 – 1,000 employees
- 1,001 – 5,000 employees
- More than 5,000 employees

ABOUT RISKONNECT

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organizations with the ability to anticipate, manage, and respond in real time to strategic and operational risks across the extended enterprise.

More than 2,700 customers across six continents partner with Riskonnect to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,500 risk management experts in the Americas, Europe, and Asia-Pacific. To learn more, visit www.riskonnect.com.

CONNECT NOW →

RISKONNECT'S INTEGRATED RISK MANAGEMENT SOLUTIONS

INSURABLE RISK

- Risk Management Information System
- Claims Management
- Billing
- Policy Administration
- Health & Safety

ACTIVE RISK MANAGER

HEALTHCARE RISK & PATIENT SAFETY

BUSINESS CONTINUITY & RESILIENCE

- Business Continuity Management
- Operational Resilience
- Emergency Notifications
- Crisis Management
- Threat Intelligence

GOVERNANCE, RISK & COMPLIANCE

- Enterprise Risk Management
- Third-party Risk Management
- Environmental, Social & Governance
- Compliance
- Internal Audit
- Internal Controls Management
- Policy Management
- Project Risk Management
- IT Risk Management
- AI Governance
- Business Strategy