

riskonnect.

The 2026 New Generation of Risk Report

Addressing the New Realities and Risks in 2026 and Beyond

Executive Summary

The Iran war disrupted global energy and shipping markets this year. Trade policy and tariffs have impacted costs, market access, and supply chains. AI continues to reshape how companies operate and their exposures.

The threats are compounding in ways that are harder to predict, rarely staying contained to the departments where they started. The risk function is straining to keep up. Seventy-five percent of risk leaders say pressure on them has increased over the past year. Thirty-seven percent say the pressure is high or extreme.

That increased pressure is not surprising since risk leaders are shouldering much more than a few years ago. They're expected to cover more ground, see further ahead, and respond faster, all without a corresponding increase in headcount or budget. Only a quarter of risk leaders saw their risk management technology budget grow in the past six months.

The *2026 New Generation of Risk Report* is based on a survey of more than 250 risk, compliance, and resilience professionals worldwide on how they and their organizations are responding to a risk landscape moving faster than ever. The report reveals that they are leaning harder into AI, rethinking what risk leadership looks like, and pushing to be seen and heard at the board level. At the same time, critical governance and risk management gaps remain even as the velocity of change intensifies.

Risk Management Jobs Are Getting Harder (and the Backing Thinner)

Risk professionals are under more pressure than ever, but support to help manage it isn't keeping pace. Seventy-five percent of survey respondents say pressure has increased on their role over the past year, with 20% calling the increase significant. Thirty-seven percent say the pressure is high or extreme.

Several forces are converging and driving this pressure on the risk function.

> *Risk leaders are caught between accelerating risk velocity and stagnating budgets. The pace at which risk moves and compounds has outrun what most risk functions were built to handle. Organizations are facing fast-moving regulatory changes, consumer sentiment shifts, mounting financial pressures, and more. At the same time, everything a company does is more visible which raises the risk to brand reputation. Risk teams are seemingly expected to keep up with all of this and protect the organization without getting more resources to do it.*
>
> **Jim Wetekamp,** *CEO*, Riskonnect, Inc.

Only 25% of survey respondents say their budget for risk management technology has increased in the past six months. The majority (66%) said their budgets have stayed the same, a slight increase over previous years. This is a clear indication that investment isn't keeping pace with higher expectations, an escalating workload, and the needs of a function that's only grown more strategically important.

Risk teams are finding ways to make their value visible. When asked what actions they're taking to help the board and executive leadership team understand risks and the impacts, survey respondents point to a few clear tactics:

- **66%** are making risk information and reports easier to understand.
- **59%** are linking risks directly to business priorities, strategy and performance.
- **56%** are focusing on top priority or new risks instead of all likely risks.
- **44%** are quantifying the potential business or financial impact of key risks.



Despite the pressure, risk professionals still love the job. Eighty-six percent say they would recommend a career in risk management to a family member or friend based on their personal experience working in risk management over the past year and their outlook for the future. This is a sign the work still feels valuable and strategic even as the job gets harder.

A Risk from Within: Silos Are Still Plaguing Companies

Stagnant budgets and resources aren't the only internal challenges risk teams are up against. Siloed decisions are adding to the pressure.

Forty-one percent of respondents say that in the past year, a department in their organization made a risk-based decision without consulting the risk team that had a significant, unforeseen disruption on a different area of the organization.

Getting ahead of this cascading effect is two-fold. First is awareness: Foster a culture where every department knows when to loop in the risk team. Second is visibility: Create a connected view of risk that brings all risk domains into one picture so risk teams can catch what's forming, proactively act, and respond faster to changing conditions.

41%

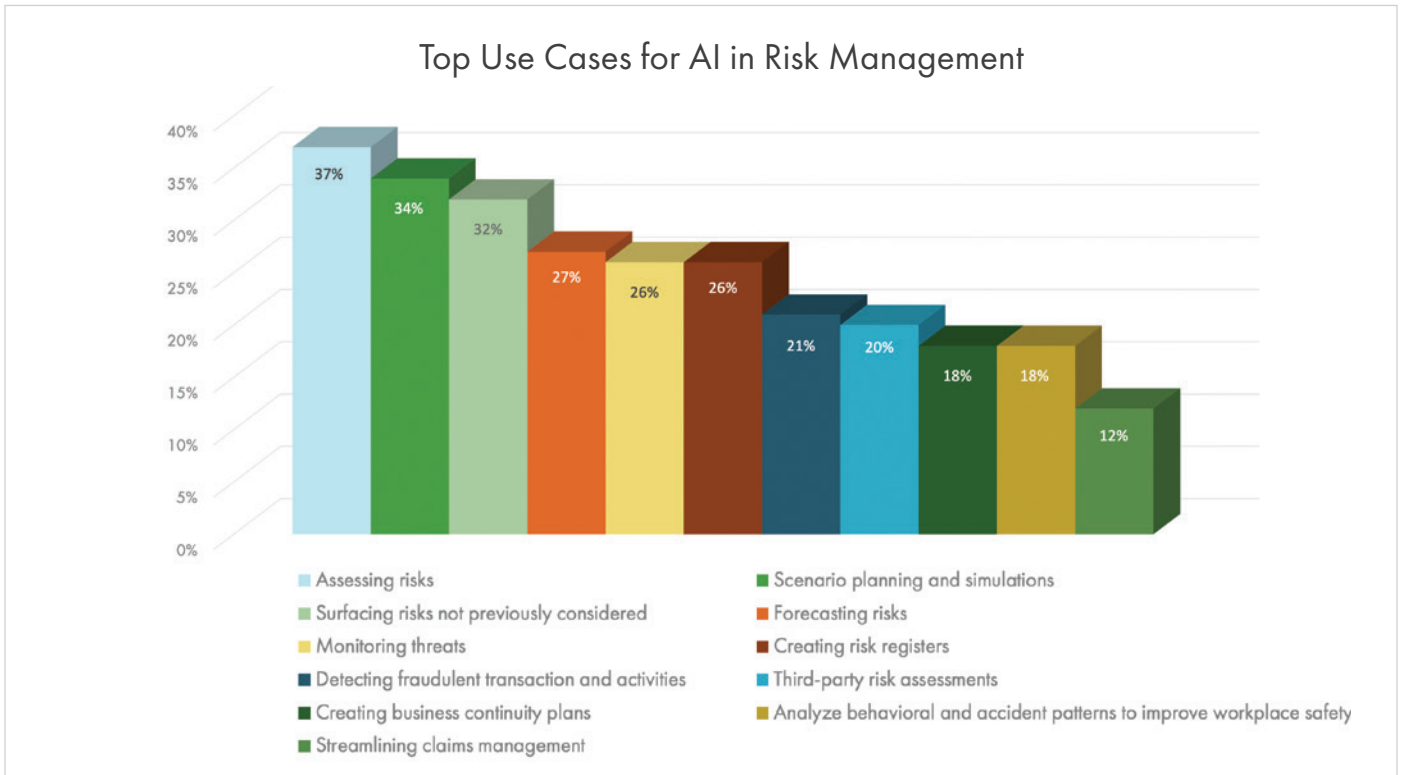
of respondents say another department has made a risk-based decision in the past year without consulting the risk team that had a significant, unforeseen disruption on a different area of the organization.

Risk Teams Lean into AI to Punch Above Their Weight

With more to do – when budgets and resources are standing still – risk leaders are using AI as a power multiplier to see more, move faster, and adjust confidently the moment conditions change.

Seventy-four percent of respondents indicate they currently use or plan to use AI for risk management, up from 70% last year and 62% in 2024. Top AI use cases include:

- **37%** Assessing risks
- **34%** Scenario planning and simulations
- **32%** Surfacing risks they hadn't previously considered
- **27%** Forecasting risks
- **26%** Threat intelligence to monitor threats to people and operations
- **26%** Creating risk registers



AI is also helping risk leaders identify a risk or vulnerability that would have been difficult to detect on their own. Thirty-one percent of survey respondents say AI has helped them uncover gaps or weaknesses in internal processes or controls in the past 12 months. Other ways AI has helped include identifying patterns or anomalies in large or unstructured data sets (25%), highlighting connections between risks that were not previously visible (22%), and detecting emerging or previously unrecognized risks (21%).

How Risk Is Measured

Risk quantification is another way risk teams can enhance their ability to keep up with today's environment. When asked about the methods their organization uses today to quantify risk:

59% use heat maps.

51% use financial impact modeling (such as expected loss or value at risk).

44% use scenario analysis or stress testing.

18% use Monte Carlo simulations.

15% rely on judgement rather than formal quantification methods.

When it comes to keeping up with regulatory changes, 74% of respondents say their organization uses manual monitoring by internal compliance staff. Only 11% use automated regulatory change-management tools. Other ways companies stay on top of regulatory changes include:

63% use industry association memberships and alerts.

61% use subscriptions to legal or regulatory update services.

48% use external counsel or advisors.

Risk Leadership Is Shifting from a Seat to a System

Just over half (53%) of companies have a chief risk officer. Of those that don't, 92% say they have no plans to hire one in the next 6-12 months.

The number of companies with CROs hasn't meaningfully changed over the past four years. That doesn't necessarily mean risk representation at the leadership level is stalling. Rather, it could be changing shape. Instead of centralizing risk ownership to a single person, more companies appear to be focusing on building a single, integrated view of risk where ownership sits with a risk committee and connected technology keeps everyone working with the same facts, using the same language, and measuring status with the same metrics.

> *Risk is a matrixed function at many organizations. We're seeing more companies express a desire for a single view of risk vs. centralizing risk leadership in a single role. This often looks like a risk council where business partners – including the head of business continuity and resilience, internal audit, insurable risk, compliance, and others who are out in the business and understand how it operates – come together for a shared view of risk. Regardless of the structure or approach, what matters most is that authority and alignment are operationally built.*
>
> **Jim Wetekamp**, *CEO*, Riskonnect, Inc.

Economic Risk Catches Up to Cyber as a Top Corporate Threat

Cybersecurity's two-year reign as the #1 business risk just ended in a tie. Economic risk has caught up, with the percentage of risk leaders saying economic risk is having a severe or significant impact on their business now level with cybersecurity at 55%.

Cybersecurity risks are still a real threat, but economic risk climbed in the past year with tariff shocks, persistent inflation, and a cooling labor market.

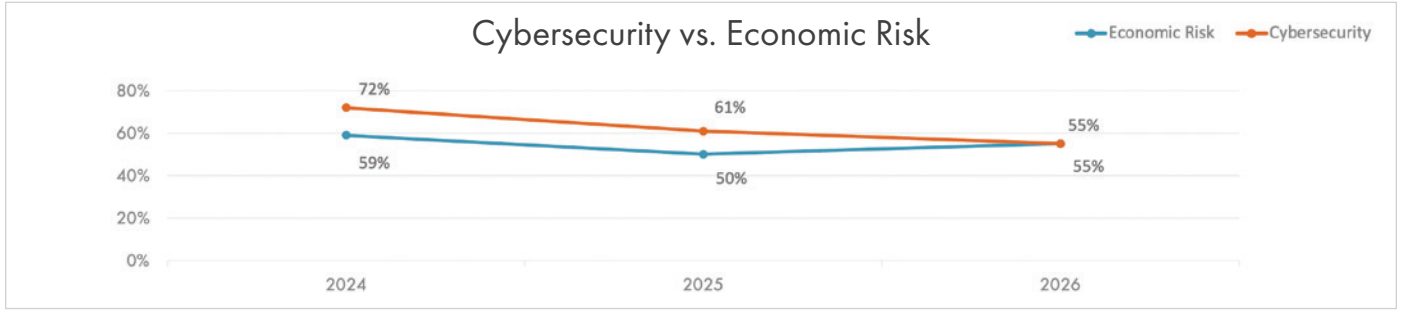
Other top risks identified by respondents as having a severe or significant impact on their business are political risks (38%), geopolitical risks (37%), and talent risks (37%). All are hitting at once, which underscores the pressure risk teams are under as they manage a wide field of threats.

Talent Risk Creeps Back into the Top Five

Talent risk edged back in the top five this year. This shift tracks with a labor market pulled in multiple directions. AI is reshaping work and which roles companies need. Skills shortages are a real challenge. And a slower economy is encouraging talent to stay put instead of switching jobs, making it harder for companies to hire. Only 20% of respondents report being very prepared for talent risks.

Top Five Risk Drivers

	2026	2025	2024	2023
Cybersecurity Risks	#1	#1	#1	
Economic Risks	#1	#2	#2	#2
Geopolitical Risks	#3	#5		#5
Political Risks	#2	#3	#4	
Talent Risks	#3		#3	#1
Third-party & Nth Party Risks			#4	
Ransomware & Security Breaches				#3
State-Sponsored Cyberattacks				#4
Supply Chain Risks		#4		

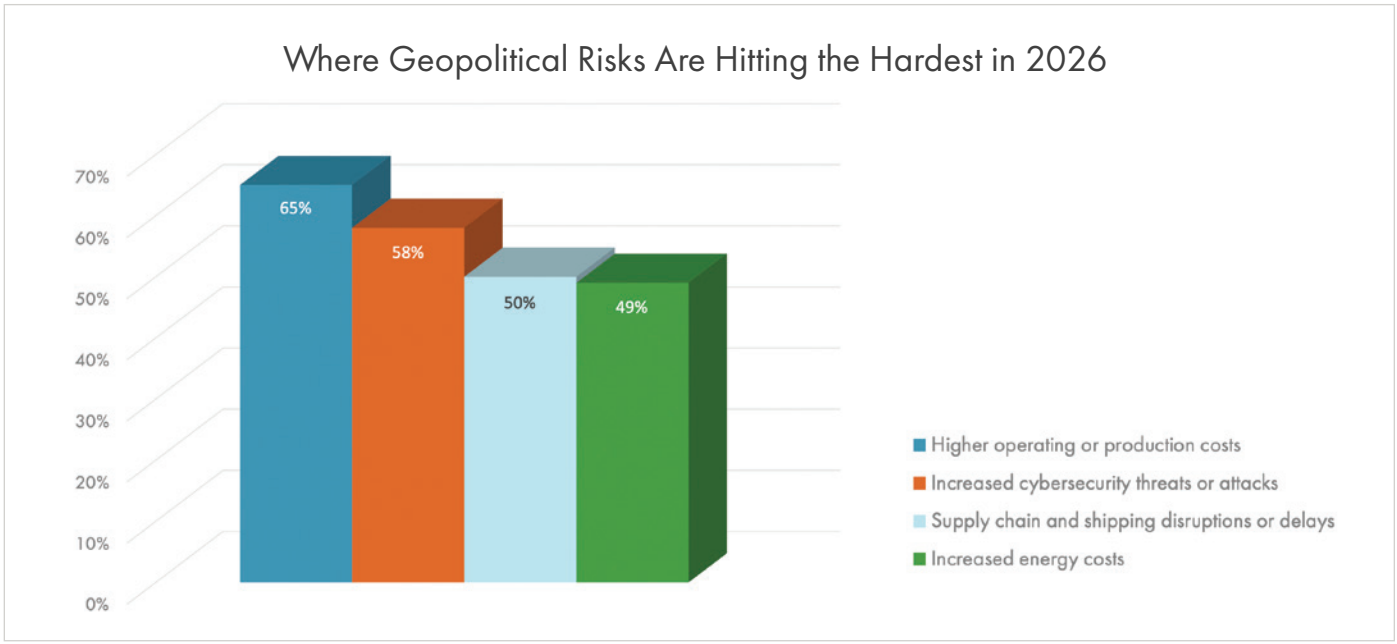


Geopolitical Risk Persists

Geopolitical risk remains a top threat. When asked about which events or vulnerabilities had the most significant impact on their organization in the past year, 40% of respondents said the Iran war, ahead of the Red Sea shipping attacks (5%), extreme weather events (31%), major cloud outages (24%), and other events. Of those that ranked the Iran war at the top, only 1 in 4 reported they were ready for all the impacts of the event. Survey respondents said they were least prepared to manage the following secondary or cascading impacts: energy shortages and price volatility (20%), supply shortages and inventory stockouts (14%), and increases in logistics and transportation costs (14%).

Fifty-eight percent of respondents say they had a plan for geopolitical volatility heading into 2026. Of those, 31% said the impact was worse than they expected. Just 19% of survey respondents said they are very prepared to assess, manage, and recover from geopolitical risk – essentially flat over 2025.

This picture points back to risk velocity and how difficult it is to stay ahead of these risks. Agility is what matters most in this environment.





What separates the companies that recover quickly from the ones that don't is whether they understand their risk landscape well enough to adapt on the fly. This means knowing in advance where key suppliers and customers are located, what their core processes are, and what the business depends on to keep running. Planning still matters, but having the right data at your fingertips to move fast is what separates a manageable moment and fast recovery from a lasting hit.

AI Governance Continues to Lag

AI governance gaps are showing up in three key places: Company policies on what tools are approved, when to use them, and training employees on how to use them responsibly.

More companies have AI policies, but they only go so far

Seventy-two percent of respondents say they have a policy governing AI use by employees, up sharply from 58% last year. But the data indicates these policies are stopping at the surface. Only 54% of respondents say they have clear policies and guidelines on what AI tools can be used and how they can be used. That indicates a sizable minority is left to figure things out on their own.

That gap matters because risk leaders have clear opinions on which AI tools are lower risk. When asked to rank large language models – including ChatGPT, Claude, Copilot, Gemini, Grok, and Perplexity – by perceived risk to the organization (with 1 representing lowest risk and 6 highest risk), Copilot is considered lowest risk, with 64% rating it a 1 or 2, followed by ChatGPT (54%) and Claude (39%).

Risk leaders are making judgments on specific AI tools and governance must go deeper than a blanket AI policy.

Only:

- **31%** have a policy against using foreign AI models like DeepSeek.
- **30%** have a policy in place to govern the use of AI by partners and suppliers.
- **23%** have a dedicated plan to specifically address AI risks, including but not limited to deepfakes and AI-driven fraud attacks.
- **11%** have a budget specifically directed at mitigating AI-related risks.

Most companies weighing agentic AI haven't assessed the risk

Most respondents indicate their companies are somewhere on the agentic AI adoption curve, saying they've either already incorporated (27%) or are considering (56%) incorporating agentic AI solutions into the organization's operations or products.

Among those that say their companies have already incorporated agentic AI, 84% say they've assessed the risk, though that number should arguably be 100% for a technology already live within the business. Among the much larger group still considering it, the majority (58%) haven't assessed the risk.

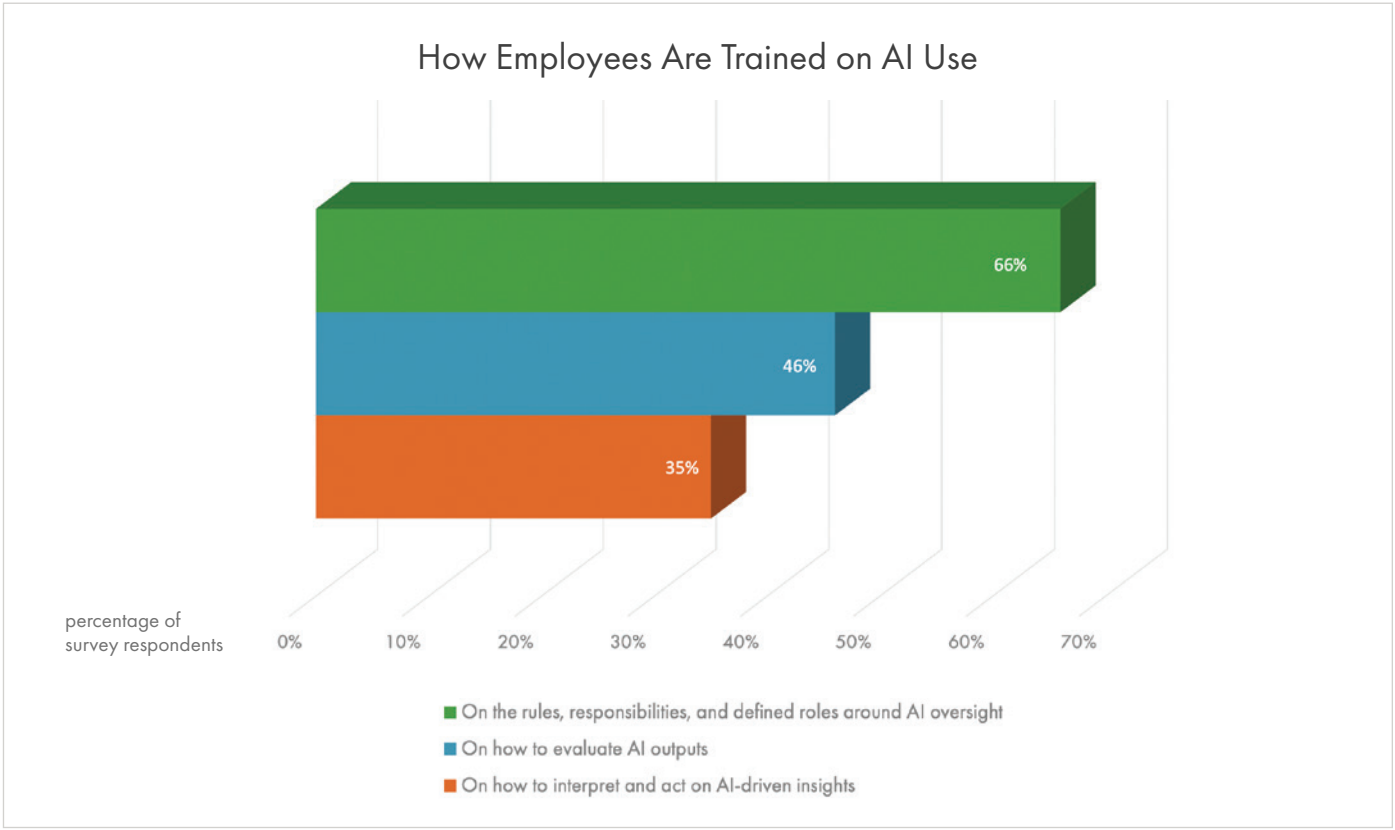
Moving fast on agentic AI doesn't mean skipping the conversation about risk. Companies that build risk into the evaluation and decision process from the start are in a better position to capture the value agentic AI can deliver while staying ahead of what it can get wrong.

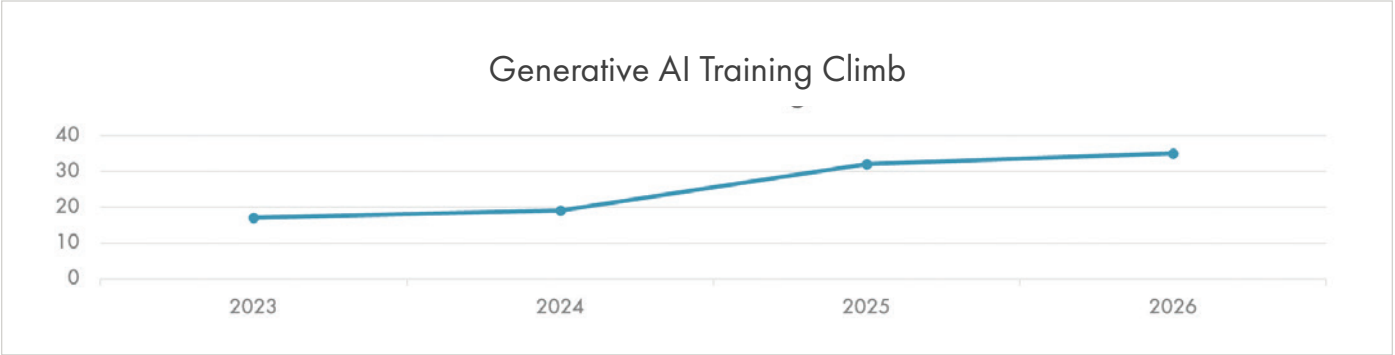
Organizations aren't teaching employees to use AI effectively

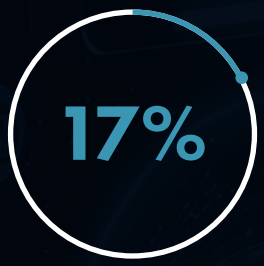
Less than half (46%) of respondents say employees at their company have been trained on how to evaluate AI outputs (in terms of what to trust versus challenge). Just 35% say their companies have trained employees on how to interpret and act on AI-driven insights.

Training also lags when it comes to governance and managing the risks of AI. While 66% have trained employees on rules, responsibilities, and defined roles around AI oversight and accountability, just 18% have formally trained or briefed the entire company on risks related to agentic AI.

Even generative AI, which has been on the mass market longer than agentic AI, has only reached 35% in terms of companies that have done formal and company-wide training on the risks. This number has climbed slowly from 17% in 2023.







How to Think About AI Governance: Building Blocks for a Strong Foundation

Only 17% of risk leaders feel very prepared for AI and AI governance risks. Sixty-two percent say they feel somewhat prepared.

AI adoption, however, is not waiting for the corporate green light. New tools, use cases, and integrations show up regularly. Staying ahead of the risk starts with building strong guardrails that consider the bigger picture:

- Where is your organization currently using AI? Which tools are in use, in which functions, and who is making the call to use them?
- What's your process for evaluating a new AI tool before it's brought in?
- How are you tracking how the AI tools we use change over time?
- Which outside partners and AI model providers sit behind those tools? Do you know the full list?
- How does the AI tool make its decisions?
- What level of autonomy do you want the tool to have and where should human oversight kick in?
- How does the AI tool fit into the core business processes?
- Who oversees the AI tool?
- If the AI tool stops working, what happens? Do you have a continuity plan?

Bringing in a new AI tool deserves the same scrutiny as hiring a new employee. Is it trustworthy? Do you understand its decision making? Is it ethical? Can it do the work you expect it to? Does it deliver with confidence? Similar to how you wouldn't hire someone and never check in again, continuously reassess AI's performance, especially as tools update. Watch for drift. Assign someone to be accountable for how each tool is performing over time.

Risk Management by the Numbers

Worst-case scenario planning:

55%
say they've simulated their worst-case scenario.

88%
of those that have simulated their worst-case scenario say they've simulated it in the past 12 months.

Spreadsheet use:

49%
mostly or only use spreadsheets to manage risk.

51%
mostly or only use dedicated software.

Data confidence:

21%
say they are very confident in the accuracy, quality, and actionability of their risk management data.

71%
say they're somewhat confident (YoY trend: 65% in 2025, 63% in 2024, 59% in 2023).

8%
say they aren't confident (YoY trend: 10% in 2025, 16% in 2024, 17% in 2023).

Steps companies are taking to prepare for crisis scenarios:

74%
Collaborating with cross departmental stakeholders (YoY trend: 65% in 2025, 62% in 2024)

73%
Regularly reassessing our risks

66%
Regularly updating business continuity plans

61%
Participating in tabletop exercises (YoY trend: 57% in 2025, 55% in 2024)

61%
Involving leadership in planning and testing for unexpected crises

57%
Regularly reassess crisis response plans

4%
Not taking any steps to prepare for a crisis (YoY trend: 7% in 2025, 8% in 2024)

Evolve Your Playbook

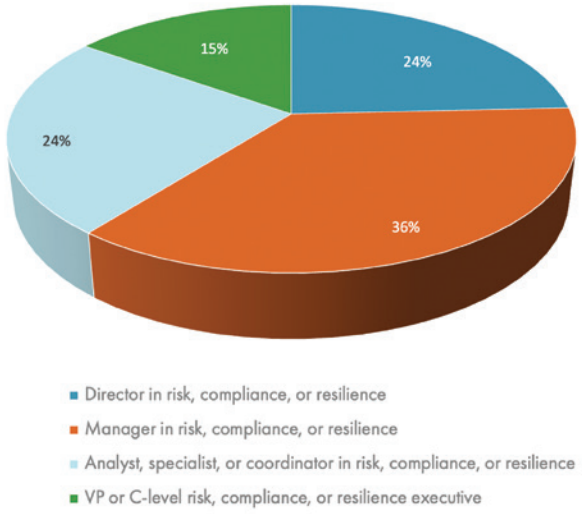
The biggest risk in today's environment may be standing still. Companies that will thrive have a solid foundation of risk knowledge at the ready, allowing them to instantly pivot with conditions.

A few steps to take now:

- Make your impact visible to the board. Connect risk directly to business priorities and let that visibility make the case for more budget and resources.
- Build agility. Do you know your risk profile, critical dependencies, priorities, and strategic goals well enough that you can move the moment something happens? You don't want to waste time gathering information in the heat of the moment.
- Supercharge your risk team with AI. Leveraging AI is key for boosting the power of a small risk team in a fast-moving environment. Put intelligence at your fingertips so you can respond to risk faster.
- Close AI governance gaps. Don't take your hands off the steering wheel. Govern AI like any other risk. Teach employees when to trust what AI tells them, when to challenge, and how to validate results. Deploying a tool isn't the same as preparing people to use it well.
- Invest in technology that is built for the practitioner by practitioners. The right tools enable risk teams to move as fast as the risk itself and make the job more manageable in an environment that keeps getting tougher.

Demographics of the 259 risk, compliance, and resilience professionals who responded to the survey.

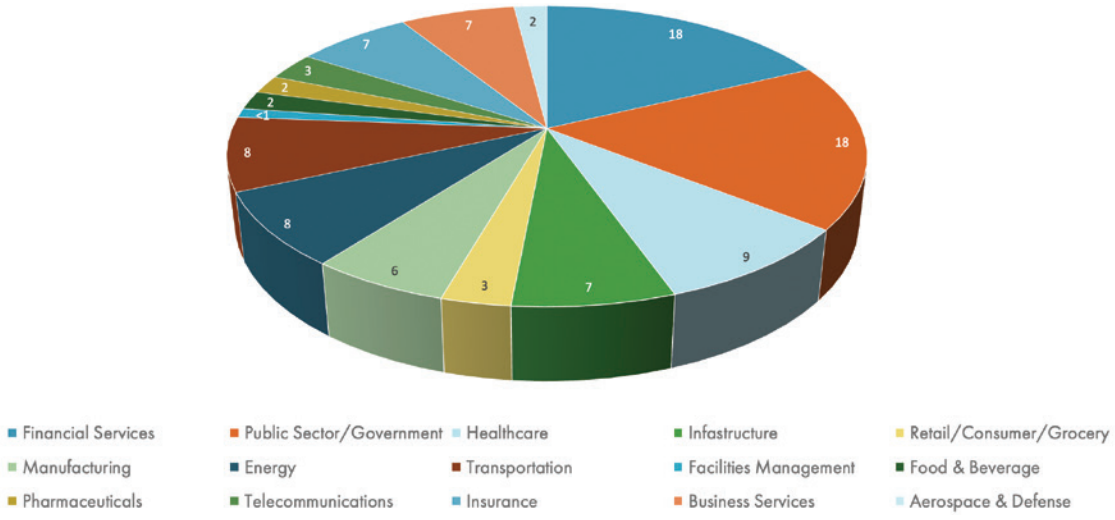
Role



Company Size



Industry



Start anywhere. Expand everywhere.

Riskonnect is the leading provider of software that brings risk under one roof. The technology empowers organizations 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 riskonnect.com.

INSURABLE RISK | GOVERNANCE, RISK & COMPLIANCE | BUSINESS CONTINUITY & RESILIENCE

riskonnect.

Copyright © 2026 Riskonnect, Inc.
All rights reserved.