riskonnect

The 2024 New Generation of Risk Report

ADDRESSING THE NEW REALITIES AND RISKS IN 2024 AND BEYOND

Executive Summary

Geopolitical tensions are escalating. The economic outlook keeps flip flopping. But the dominant story this year is AI.

Concerns over AI ethics, privacy, and security continue to mount. AI also tentacles into cybersecurity, geopolitics, and other areas, supercharging the risks of everything in its path. Hackers, for instance, are getting smarter, more sophisticated, and dangerous by the minute as they leverage the latest AI advancements to infiltrate organizations.

These forces are creating a high-stakes environment full of challenges to navigate. Are risk management strategies keeping up with this new generation of risk?

Riskonnect surveyed more than 200 risk, compliance, and resilience professionals worldwide to uncover today's biggest threats and if organizations' risk management playbooks are ready for the uncharted territory.

The 2024 New Generation of Risk Survey reveals that while companies' top concerns have shifted over the past year, risk management approaches largely haven't evolved fast enough and key gaps remain. The data also suggests that risk management is increasingly seen as a strategic business function, but continued investment is necessary to keep up with the changing risk landscape.

Cybersecurity Threats: The Foremost Concern

Cybersecurity is now organizations' number one risk driver, surpassing economic risks and talent challenges, which were the top two drivers in 2023. Seventy-two percent of respondents said cybersecurity risks are having a significant or severe impact on their organization. This is a notable increase from last year (47%), which highlights the growing urgency to address these threats.

The fact that cybersecurity risks top the list isn't surprising. AI-powered cybersecurity threats – ransomware, phishing, deepfakes – are rising. In fact, 24% of respondents said that over the next 12 months, these threats will have the biggest impact on their businesses.

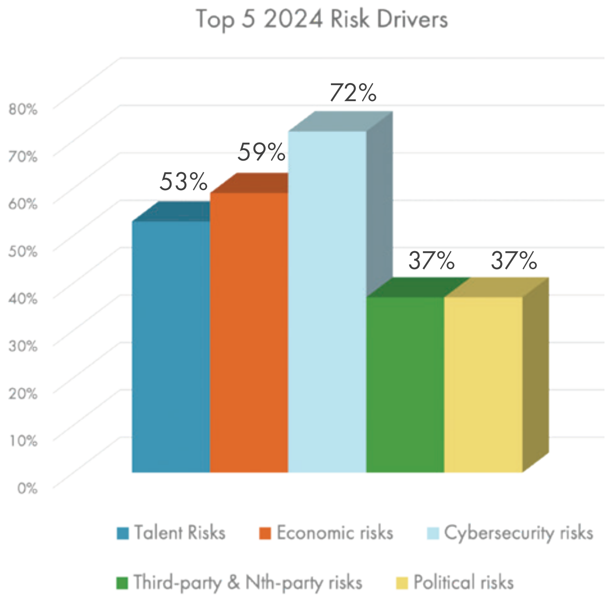
What is surprising is that most organizations (80%) don't have a dedicated plan to address generative AI risks, including AI-driven fraud attacks, which go hand in hand with cybersecurity. Sixty-five percent of companies don't have a policy in place to govern the use of generative AI by partners and suppliers.

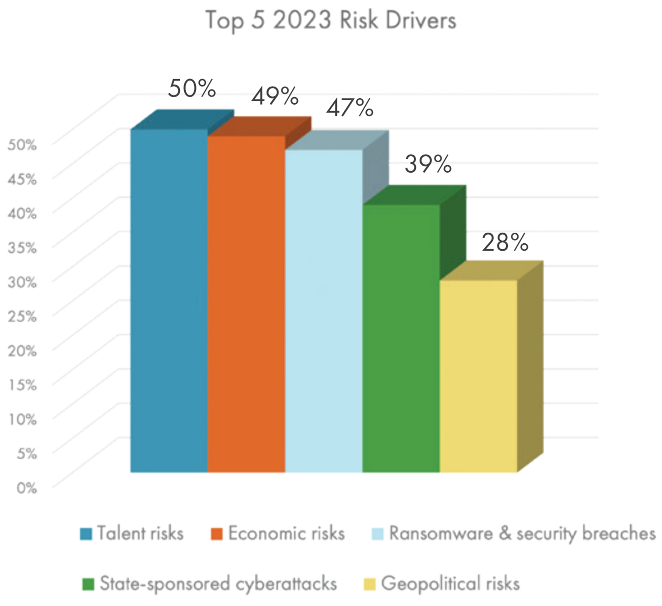
Companies put a lot of time and money into cybersecurity. But if they aren't factoring generative AI and third-party risks into their cybersecurity risk management approach, then they are still significantly exposed.

> *"If you don't have a plan for generative AI and third-party risks, you don't have a cybersecurity plan. AI risk is cyber risk. Cyber risk is third-party risk. These risks are also ever-changing in nature. You might feel prepared for what's out there today, but the landscape will change – and fast, says Roger Dunkin, co-founder and chief strategy officer at Riskonnect."*

Other risks cited as having the biggest impact on businesses over the next year include the U.S. presidential election (15%), interest rates and inflation (14%), and increased government regulation and oversight (14%).

Riskonnect's data suggests that companies can't advance their own practices at the pace cybercriminals are advancing theirs and are waiting for the government to step in. Sixty-three percent of respondents said risks related to AI-driven fraud and manipulation tactics would be most important for AI regulation to address.





Generative AI Risks: A Growing Challenge

Despite the rising prominence of generative AI, companies' confidence and action in addressing these risks is stagnant compared to last year. Only 8% feel prepared for AI and AI-governance risks. Just 19% of organizations have formally trained or briefed their entire organization on generative AI risks.

Other key findings include:

- 59% say leadership doesn't actively guide and support enterprise generative AI initiatives and governance with actionable plans and strategies.
- Only 16% say they have a budget specifically directed at mitigating AI-related risks.

Companies' inaction against generative AI risks likely stems from not knowing where to start or how to best direct resources given these threats are constantly evolving. While the absence of training and top-level engagement can impede effective risk management and governance, it's quite possible the lack of executive support is unintentional. Senior leaders might not know any more than staff about these risks, leading to a lack of guidance and budget.

Pull in the risk managers

Only 20% of risk management teams say they are always involved in decisions about incorporating AI into operations, products, or offerings, such as decisions to implement dynamic or surge pricing. The lack of inclusion of risk management teams in these types of decisions is likely a result of not training and equipping staff across the organization on generative AI risks, including when and why to pull in the risk department. This is problematic as organizations' AI adoption grows.

> Think about the advent of email. Organizations ultimately needed to create policies around its use. These policies specified that employees shouldn't put sensitive information in email and should understand emails are archived, searchable, and legally discoverable. As generative AI adoption grows and more departments consider leveraging these tools, the same type of policies and guidelines need to be in place.

At a higher level, risk leaders also need a seat at the table as companies seek ways to drive business value with AI. Every strategic decision a company makes creates risks. Risk leaders are instrumental in ensuring these risks are acknowledged and controlled. They can help ensure that AI is used in a way that advances strategic objectives instead of exposing the company. Risk representation at the C-level is holding steady over last year: 52% of respondents say their organization has a chief risk officer.

AI's Impact on Jobs: A Positive Outlook

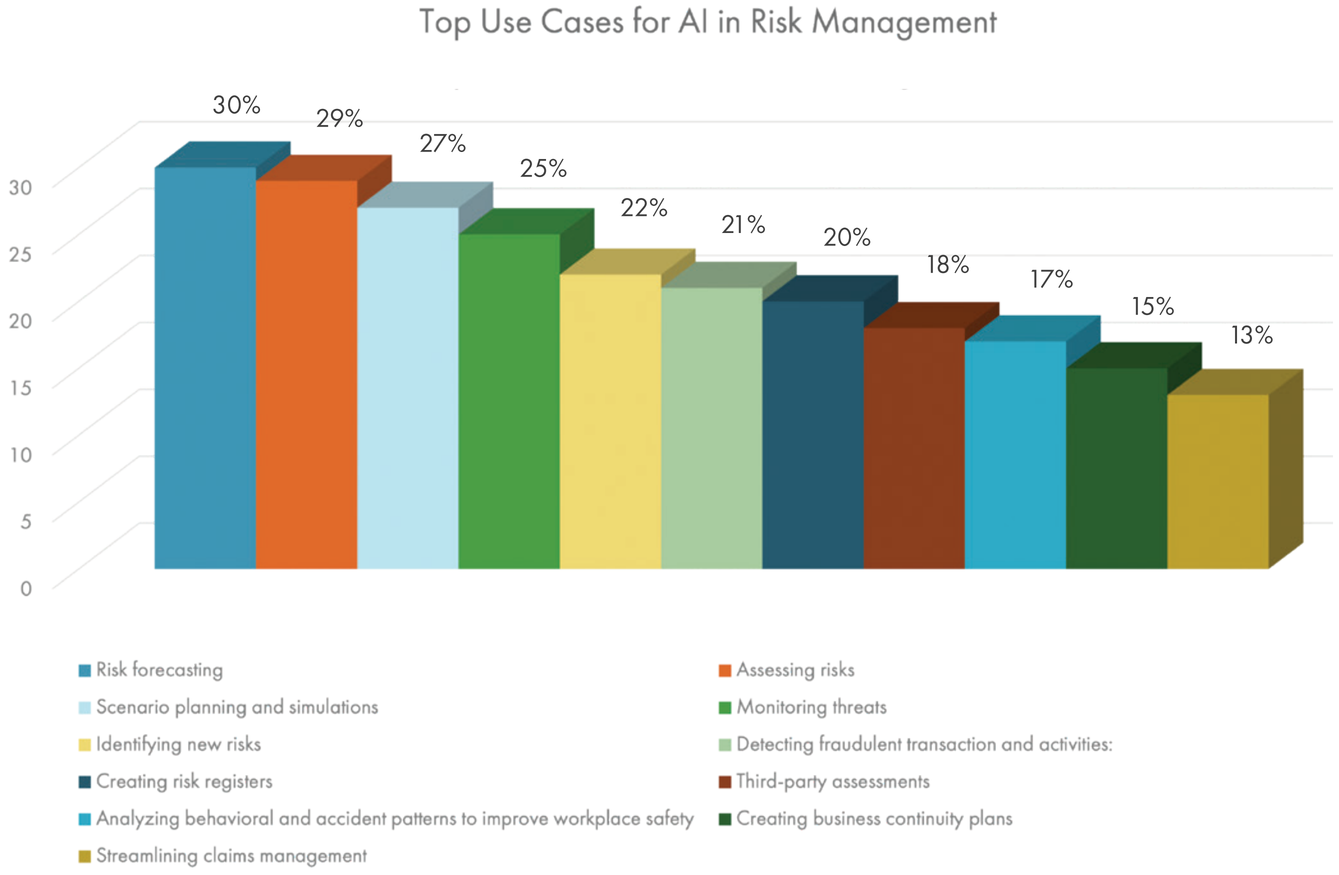
Naturally, when companies adopt AI, employee fears of job replacement arise. However, the impact of AI on risk management jobs remains positive. Only 5% of companies plan to reduce their risk management, compliance, and resilience workforce in the future because of AI – which is a testament to the strategic value of risk departments. The data indicates that organizations overall view AI as a tool to enhance, rather than replace, risk management roles.

In fact, the top driving force for technology adoption is equipping risk, compliance, and resilience teams to be more efficient and focus on strategic work (62%). Better visibility into risk to effectively manage threats (60%) and increasing the department's performance and business contributions (40%) were close behind.

62% of companies currently or plan to use AI in risk management.

Ninety percent of companies have increased or maintained their risk management technology budgets – another proof point that risk management is a strategic function that companies are investing in.

The strategic use of AI in risk management can enhance the risk management team's efficiency and performance. By automating routine tasks and providing advanced analytical capabilities, AI enables risk management professionals to focus on higher-value activities and strategic decision-making.



Geopolitical Risks: A Prevailing Threat

Only 18% of respondents say they're prepared to handle geopolitical risks.

Sixty-one percent of organizations do not have a plan for managing risks and disruptions related to future geopolitical tensions, such as a potential conflict between China and Taiwan. Just 20% of those companies say they're in the process of creating one. And another 20% of companies "aren't sure" if they have a plan.

This gap in preparedness is concerning, given the current geopolitical climate, the likelihood of future events occurring, and the substantial impact geopolitical situations can have on the enterprise. Talks of a Chinese invasion of Taiwan, for example, are escalating, and the scale could be worse than the Russia-Ukraine war.

The first thing many companies think of when it comes to the impact of geopolitical situations is the supply chain. The ongoing conflict between Russia and Ukraine, for example, created severe food shortages and inflation around the world. But the impacts of geopolitical events can also manifest in many other ways, including shifting regulations, changes to tax rules and employment laws, cyberattacks, market volatility, and boycotts and public backlash. The impacts of one geopolitical event can cascade and have far reaching consequences across the enterprise. And companies need to be ready.

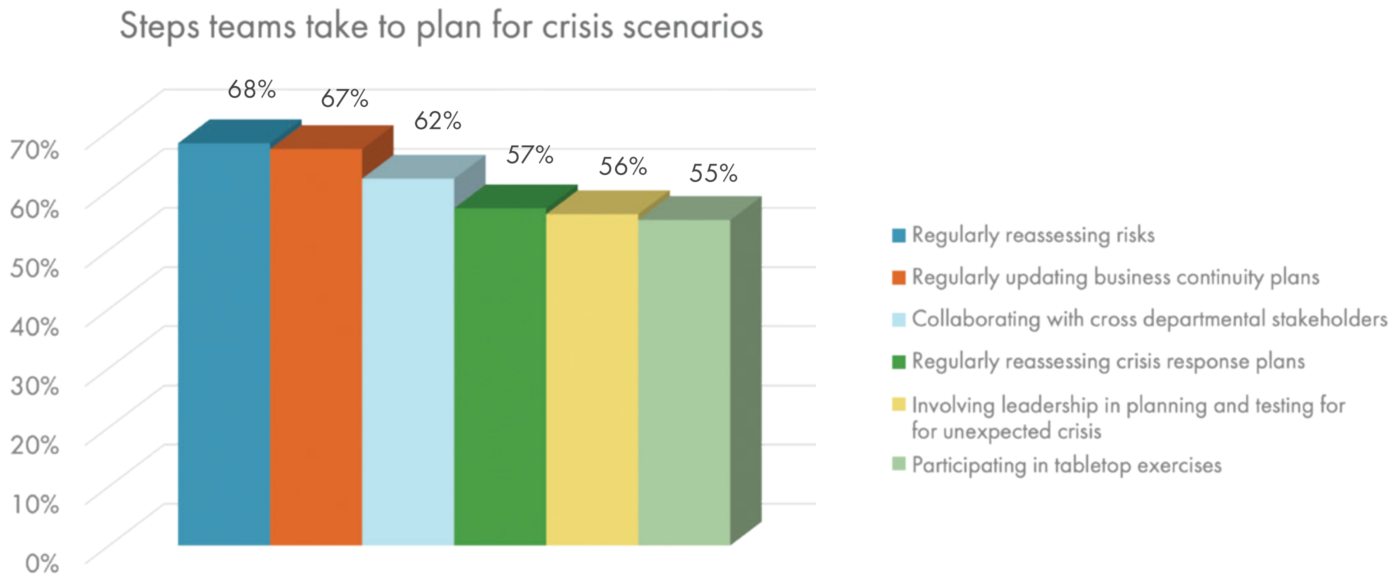
Scenario planning is a valuable practice for preparing for potential geopolitical events. Yet in 2023, most organizations (63%) surveyed had not simulated their worst-case scenarios. Most respondents had said their worst-case scenarios revolve around geopolitical risks, cyber, and natural disasters. This year's research uncovers that companies haven't made significant moves in the past 12 months to close the gap in scenario planning.

Scenario Planning: A Gap Remains

Over half (56%) of companies today have not simulated their worst-case scenarios. This, along with the lack of plans for managing future geopolitical tensions and disruptions, is shocking considering geopolitical events were commonly cited as worst-case scenarios again this year and the current world events in Russia-Ukraine and the Middle East.

Companies also could be doing more to strengthen their preparedness for unpredictable events. Only 4% say they're prepared to manage a future unknown and unpredictable risk event (compared to 5% last year).

Most (92%) companies are, however, taking other steps to prepare for crisis scenarios.



Some crises, however, are simply too big to plan for. AI is helping risk managers identify the major risk events that are outside of their control, such as nuclear war or pandemics, that are too big to plan for. That way they can allocate their time toward planning for the situations where they will have more of an impact.

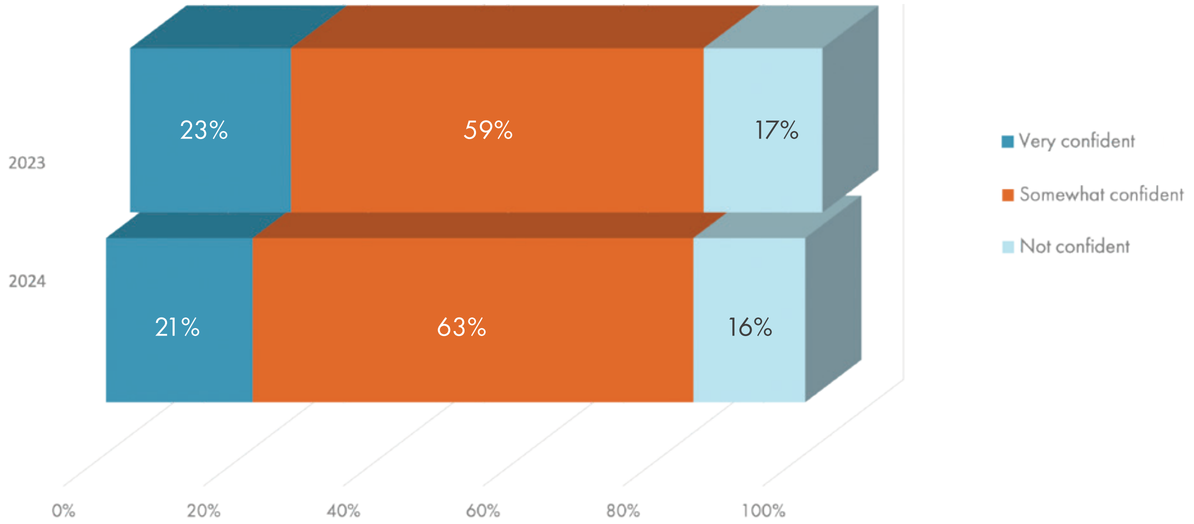
> *Building general resilience in the system is also critical for getting through any high-risk, high-impact event. Focus on your financial position, debt, relationships with your contract workers, and other factors in your control. These are things you can fall back on and will help you get to the other side of a crisis, says Jim Wetekamp, Riskonnect's CEO.*

Spreadsheets: A Persistent Challenge

Despite advancements in risk management technology, many organizations continue to rely on spreadsheets for managing risk. Over half (53%) of companies are only or mostly using spreadsheets. More than a quarter (27%) are exclusively using spreadsheets.

The reliance on spreadsheets is leading to data integrity problems. Only 21% of respondents express high confidence in the accuracy and actionability of their risk data. Most companies (63%) say there are some gaps in the breadth, accuracy, and timeliness of their data, and they can't make confident decisions. Sixteen percent say their data can't be trusted, and they can't get real-time information.

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



Overall, companies' confidence levels in their data haven't moved much from last year. But the outlook over the next 12 months looks brighter as companies grow in their tech maturity.

Forty percent of companies say that within a year they'll have made some investments in risk management tools. Twenty-five percent say they will have actively adopted modern risk management software, and 20% will have dedicated risk software that is integrated with other functional areas in the organization. Still, 16% say they will continue to exclusively use spreadsheets.

Revamp Your Playbook

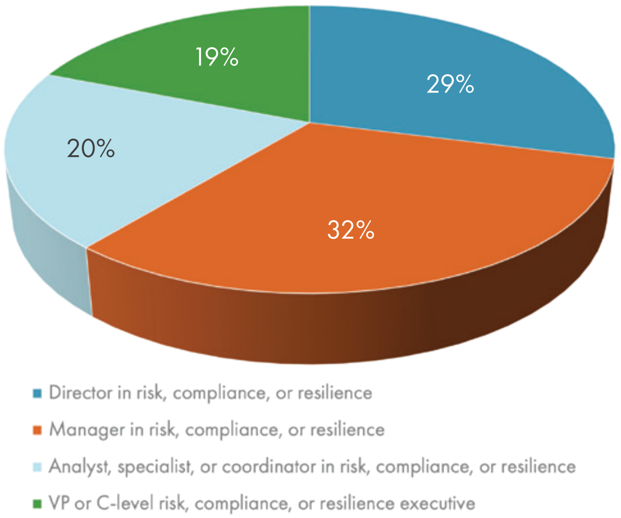
Riskonnect's research indicates that risk management strategies aren't evolving fast enough to keep up with the growing threat landscape. Think of risk management as a team of athletes. The more you practice and refine your strategies, the better you get at staying on top of the dynamic risk environment and protecting your organization.

A few steps you can take now:

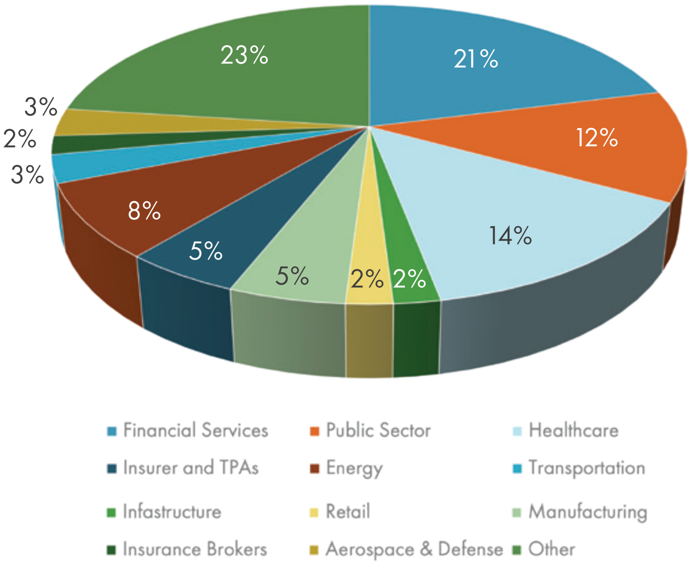
- Create an AI plan. Even if you aren't incorporating AI directly into your operations, chances are you will encounter AI risks, at the very least through phishing and other cybersecurity threats.
- Train your workforce on AI. Empowering staff to spot AI risks is critical for mitigating these threats. Equipping your team to use AI tools in the right ways enables them to work faster, smarter, and more strategically.
- Conduct scenario planning. Prepare for various crisis scenarios. Map out the resources you would need and actions you would need to take to continue operations in these situations.
- Ditch the spreadsheets. Data integrity and decision-making problems will exist as long as spreadsheets are relied on for managing risk.
- Invest in technology that helps combat the full spectrum of risk.

A total of 228 risk and compliance professionals responded to the survey.

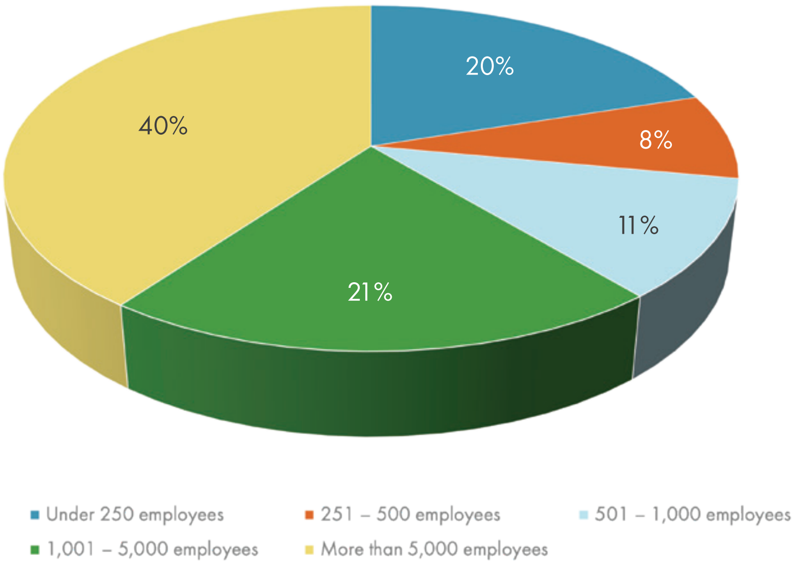
Role



Industry



Company Size



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. To learn more, visit www.riskonnect.com.