McKinsey & Company

Risk & Resilience Practice

The future of risk: How global trends are reshaping risk management

A rapidly shifting and interconnected risk landscape, technology, and AI transform what good risk management looks like. Financial institutions must embrace new operating models and best practices.

by Anke Raufuss, Arvind Govindarajan, Ida Kristensen, and Thomas Kelepouris

December 2025

Great risk management has never been more important. Considering cyberattacks, politics, and trade wars, financial institutions rely more than ever on their risk leaders to navigate uncertainty. But as the world changes, so too must risk management. Not only are risks proliferating, but so are solutions. In an AI-empowered future, new skills and capabilities will be required. Risk functions will need to be more agile, more cross-functional, and more tech-driven. In the next three to five years, executives, starting with leaders of risk functions, must embrace transformation and start to implement the required changes.

Forces at play

As risk leaders focus on building the risk functions of the future, what forces should shape their thinking? We see five that have profound implications for risk:

Geopolitical flux as the new normal. The World Uncertainty Index is nearly nine times higher than it was 20 years ago, reflecting all the geopolitical disruptions of the past few years as well as the new normal of geopolitical uncertainty.[1] Global supply chains, capital and trade flows, cyberattack patterns, and shifting domestic policies are feeling the effects of this uncertainty. In response, risk leaders will require more dynamic and forward-looking planning and forecasting frameworks flexible enough for rapidly changing environments. Activities such as stress-testing will also need to be more dynamic and consider a broader set of possible scenarios. Risk managers will need to have their finger on the pulse every day and have access to standing and response capabilities more agile than the ad hoc "war rooms" of the past.

Technological progress. Digital capabilities and AI are creating both opportunities and challenges for risk management. In onboarding, transacting, and borrowing, almost every customer journey is being reshaped by digitalization. AI is reforming the fraud and cyberthreat landscape, and contagion risk happens faster than ever. This requires access to near-real-time data and analytics about opportunities and threats creates a different talent mix to manage. Furthermore, we believe that financial institutions have to rethink risk appetite statements and frameworks for nonfinancial risks so they can to develop more appropriate risk metrics to monitor a digitally fast-moving world.

Interconnectedness of risk. Connected processes and infrastructure lead to higher levels of dependency and increased likelihood of risk contagion. Consider how geopolitical events drive supply chain disruption, which leads to credit deterioration and spikes in bond yields, or cyber events cause manufacturing shutdowns, with associated effects on credit quality and counterparty risk. Furthermore, the concentrations in technology providers increases fourth- and nth-party risks and requires a more-detailed mapping of third parties' suppliers. As risks are increasingly driven by the same underlying drivers, risk managers must break down traditional risk type silos to manage the impact of common risk drivers in an enterprise risk management function or cross-functional group.

[1] Comparing third quarter 2025 with fourth quarter 2005, "World Uncertainty Index: Global: GDP weighted average," Federal Reserve Bank of St. Louis, updated November 2, 2025.

Shifting competitive environment. The banking landscape is being reshaped by nonbankfinancial institutions (NBFIs. Indeed, the International Monetary Fund noted that the share of global financial assets held by NBFIs reached more than 50 percent in advanced economies and almost 80 percent in the United States.[2] This introduces complexity in counterparty risk management and calls for new methods to assess and oversee less regulated entities. Meanwhile, the move of many financial institutions into digital assets amplifies certain risks such as anti–money laundering and third-party risk while introducing novel risk types unique to digital assets.[3]

Fragmentation of regulations. After years of what felt like closer global regulatory coordination in financial services, we are now facing a much more fragmented regulatory landscape, with increased, although uneven, deregulation in the United States unmatched by other jurisdictions. Regulatory management and legal entity management become more complex in this environment, and simultaneously, organizations will likely increasingly find areas where internal risk appetite, rather than regulatory requirements, become the binding constraint.

What will risk management of the future look like?

The fast-changing environment presents risk management with challenges, but also with a unique opportunity to rethink the art of the possible for risk functions and for risk management overall. We believe adaptability is an imperative for risk over the next three to five years, and risk functions need to start making changes now to avoid finding their effectiveness waning.

When reinventing risk management, a tempting option is to abandon the current framework and rebuild it from scratch. But that would be a mistake. The reality is that effective change is most often a result of evolution, not revolution, encompassing both state-of-the-art capabilities and adaptations that work for the institution in question while maintaining the foundational principles of good risk management. Below we drill down into drivers of stability and change:

What will largely stay the same?

Despite all the uncertainty, certain principles and trends will continue to be important.

— *The three lines of defense (3LOD)* have attracted criticism of late, with some market participants arguing that a better approach is based on deeper business involvement, backed by technology. We believe the 3LOD model, and particularly the role of the second LOD, will remain fundamental in setting standards, monitoring adherence, and imposing accountability. Digital solutions will play a growing role, allowing the first line to efficiently take on more risk activities, but the superpowers of a good risk manager are critical thinking, intellectual curiosity, and ability to ask the right what-ifs. In a world of sometimes flawed AI, those capabilities will be more important than ever.

[2] *Global financial stability report: Financial and climate policies for a high-interest-rate era*, International Monetary Fund, October 2023.
[3] Matt Higginson and Garry Spanz, "The stable door opens: How tokenized cash enables next-gen payments," McKinsey, July 21, 2025.

— *A foundational risk management framework and a risk appetite statement* will continue to anchor risk governance, risk culture, and risk maturity. Indeed, with risks more connected than ever, and new risk dimensions emerging, risk appetite will become even more critical and will need to evolve significantly: Banks will need a more granular articulation of risk appetite, manifested in "controls by design."

— *The expansion from risk to resilience* will remain a key expectation among customers, shareholders, and regulators. It will also continue to drive a competitive advantage. In managing multiple risks, banks must embrace simplicity across processes, data and systems, and infrastructure. We expect more control via fewer controls. Cross-risk scenario analysis will be a critical tool to gauge financial resilience and operational resilience in an integrated way. Separately, among risk professionals, there is an ever-growing importance of individual resilience: the ability to be comfortable with ambiguity and take advantage of and react decisively in challenging circumstances.

What will change?

In an AI-defined future, risk management must evolve in tandem with the changing business processes it oversees. It will also need new capabilities such as continuous monitoring and built-in controls, as well as an enhanced second LOD. The transformations we expect to see include the following:

— *More dynamic risk appetite–setting and simulations reflecting greater rate of change:* To monitor their financial and operational resilience, organizations will constantly run synthetic simulations of macroeconomic shocks, climate events, cyberattacks, and other potential disruptions. Before any major decision is taken, from acquiring a portfolio to launching a product or entering a market, they will assess thousands of simulations. Potentially, banks may operate full-scale digital twins of their balance sheets and critical operations, helping them monitor their financial and operational resilience. By applying risk appetite more dynamically, banks will make faster, better-informed choices, without losing out on opportunities.

— *Continuous real-time portfolio monitoring with interventions by exception:* In the language of risk management, "assurance" is dead—or rather "periodic sample-testing assurance" is dead. It will be replaced by continuous, often real-time, monitoring as institutions plug into internal and external data ecosystems to track their exposures. In the future, the 3LODs will have access to the same data sets and will use, query, and monitor the data for their specific purposes. This will eliminate point-in-time report generation and data reconciliations, enabling faster decision-making. Risk managers will have access to automated portfolio monitoring (against the baseline) but will be able to intervene to deal with exceptions. The way we measure and manage market, liquidity, and cybersecurity risk today—continuously and at a portfolio level, with clear limits and thresholds—will be adopted for other risk types. In particular, today's case-by-case credit approval and periodic control

or key risk indicator–based monitoring of nonfinancial risks will transition. Regulators may exercise their supervision in a similar way by accessing banks' data to oversee an individual bank more effectively and to scan the financial system for systemic risks and required interventions.

— *Integrated risk profiling across risk types to assess the ultimate causes for risk holistically:* Management of financial, nonfinancial, and strategic risks will converge. Risk leaders will use data to identify the root causes of risk, both human (customers, employees, and third parties) and infrastructural (processes, systems, and data or models). Understanding customer risk, for example, will consider everything from credit history to financial crime, fraud, and cyber risk. Siloes will be consigned to history. Instead, risk functions will embrace agile, squad-based operating models, supported by risk domain experts and analytics-savvy specialists.

— *A hybrid workforce of multiagent systems and 'humans in the loop':* Risk functions will be tech-driven but human-supervised. The day-to-day operational work of risk officers (such as monitoring exposures, scoring credit, and detecting fraud) will be fully automated. The risk function will become a hybrid, with bots and agents backed by a small group of experts, a cohort of AI trainers and assurers, and "ethics stewards" to ensure transparency, fairness, and understanding of autonomous AI decisions.

— *Human risk managers equally valued for subject-matter expertise and critical orthogonal thinking.* The role of the human in the loop will shift from control to oversight. This will require the right talent to not just "check boxes" but think outside the box and ensure that automation does not create tail risks. The composition of the risk function will employ subject matter experts (for risk types and analytics) and integrative thinkers. Risk manager roles that are more process-focused will be nonhuman. To train the human workforce, we will see more adaptable, scenario- and simulation-based learning (rather than learning by doing) which will enable employees to be credible and effective humans in the loop.

Rethinking the risk function

Historically, risk functions have primarily been organized by risk types, business areas, or a combination of the two. In the future, we believe risk functions will need to be organized around three separate elements that each play a critical role. Each element will have distinct defined objectives and talent profile (exhibit):

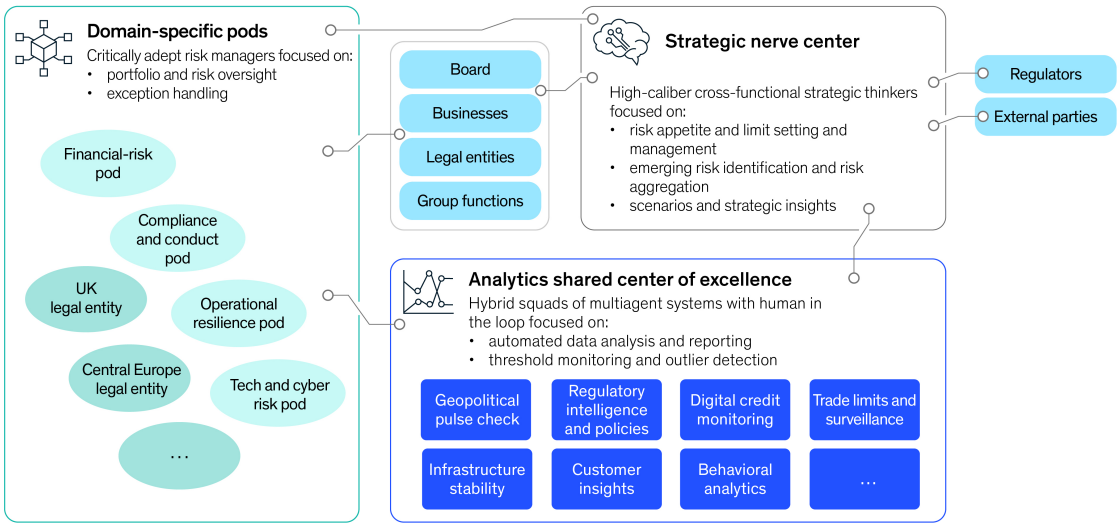
1. *Strategic nerve center.* This will be the cross-cutting intelligence unit of the risk function, in which risk appetite and limits are set, emerging risks are identified, scenarios are run, and insights are provided to the rest of the institution. The function will connect the dots between risk types and draw on analytics from a dedicated center of excellence (discussed below). The workforce will be made up of high-caliber, cross-functional, strategic thinkers.

2. *Domain-specific pods.* Pods will be organized around risk types or other critically defined domains such as material legal entities. They will be made up by senior, critically adept risk managers who will oversee the bank's portfolio of risks and apply judgment on exceptional cases. The pods will be largely business-facing, while the bulk of operational risk management and oversight will be undertaken by bots and agents. The units will be staffed by deep subject-matter experts, such as those focused on specific risk disciplines or entities.

3. *Analytics shared center of excellence (COE).* The COE should be the risk function's engine room. It will analyze vast amounts of data as it constantly monitors for outliers and threshold breaches. Activities such as reporting will be fully digitized and available via self-serve functionality. The function will consist of hybrid squads of multiagent systems with humans in the loop.

Exhibit 1

Risk functions can be organized around three separate elements.



McKinsey & Company

The organization of risk into these three elements allows for developing parallel talent value propositions, performance management, and career paths for the talent within each element. Talent in the strategic nerve center will be well trained to take on broader roles including executive leadership risk roles outside the risk function. Talent in the domain-specific pods can develop and be rewarded for deep subject-matter expertise while the analytics-based COE allows for deep data and analytical expertise. We would expect the majority of talent in the future risk function will dedicate themselves to one of the three elements, while rotational programs should exist between them to ensure sufficient cross-pollination of ideas and understanding of the interconnectedness of the elements.

What should CROs do now?

The current rate of change, both in the external risk environment and internal risk capabilities, amount to nothing less than a paradigm shift. So, how should chief risk officers (CROs) begin to build a risk function that can accommodate the more fluid and unpredictable environment? We see four immediate steps:

— *Invest in upskilling yourself and your team.* The risk function can be the biggest inhibitor or enabler of change—depending on the CRO's mindset and individual capabilities. For example, we have seen proactive, progressive risk leaders act as critical enablers for accelerated AI adoption, and those that do not. Risk leaders need to understand the opportunities and invest in educating themselves and their teams on AI, its applications, and its challenges.

— *Strengthen cross-cutting capabilities.* While risk functions may not yet be ready for the full strategic nerve center, it is critical to start addressing the need for cross-risk analysis and management. This can happen through strengthening the enterprise risk management or business risk functions of the organization or by investing in risk-agnostic monitoring and response capabilities to stay ahead of the shifting risk landscape.

— *Ensure responsible and transparent AI use.* CROs should spearhead the design and deployment of risk management mechanisms for AI. These will include clear governance frameworks for AI use-case approval and monitoring and AI processes that appropriately triage based on AI risk characteristics to ensure that the organization can solve for both safety and speed. Transparent documentation and ethical guidelines will safeguard firms against regulatory breaches and ensure that AI-driven decisions remain consistent, auditable, and aligned with enterprise values.

— *Evolve talent strategy and hire for the future.* The future of risk demands a new blend of positions, including data scientists, risk modelers, engineers, and AI specialists. CROs should assess gaps, design targeted upskilling programs, and rethink hiring, career paths, and talent management accordingly.[4]

[4] Farah Dilber, Ida Kristensen, Maxwell Yee, and Nitika Mummidivarapu, "How chief risk officers can build the next generation of leaders," McKinsey, December 10, 2025.

McKinsey recently identified three CRO archetypes—the protector, the architect, and the business accelerator—and discussed how great CROs proactively identify when they need to shift from one archetype to another.[5] In an environment where change is fast-paced, CROs may feel the need to be protectors; however, CROs must also be architects to address the required changes. By focusing on the opportunities ahead, risk managers have a unique chance to create lasting impact on the future of risk management.

Anke Raufuss is a partner in McKinsey's Sydney office, **Arvind Govindarajan** is a partner in the Boston office, **Ida Kristensen** is a senior partner in the New York office, and **Thomas Kelepouris** is a partner in the Athens office.

The authors wish to thank Cristián Berner, Cristina Catania, Daniela Gius, Monami Bagchi and Shobhit Awasthi for their contributions to this article.

[5] Cristina Catania, Ida Kristensen, Marc Chiapolino, and Tijana Trkulja, "Which chief risk officer archetype are you?," McKinsey, May 6, 2025.