

Risk & Resilience Practice

Navigating shifting risks in the insurance industry

How insurance chief risk officers balance today's complex demands.

By Erwann Michel-Kerjan and Lorenzo Serino



Today's insurers are exposed to multiple risks, from financial risks, such as shifting interest rates, changing costs and sources of capital, and increasing claims levels due to consecutive years of significant inflation, to an array of nonfinancial risks, including extreme climate events and generative AI (gen AI). This uncertain environment has spurred leaders to be more cautious but also more innovative in a way that still supports a path to sustainable, profitable growth.

The industry is taking multiple steps to manage both financial risks and pervasive nonfinancial risks. We know this based on our ongoing conversations and work with insurers and on insights gathered in our recent industry benchmark¹ of carriers (representing over \$400 billion of revenues) and at the McKinsey 5th Annual Insurance CRO Roundtable—an event attended by 25 chief risk officers (CROs) of leading life and property and casualty (P&C) insurers.

The majority of participating CROs said that they expect a slight economic downturn in the next two years and predict GDP will contract by approximately 1 percent, alongside a gradual normalization of annual inflation rates to about 2 percent. A few CROs expressed concerns over a more severe economic contraction, anticipating a GDP decrease of 3 percent or more. It's clear that capital management and balance sheet management have become even more critical for many carriers, as we further discuss below.

Beyond macroeconomic pressure, CROs are working more closely with their CEOs and boards to brace against nonfinancial threats. These leaders face growing geopolitical instability and uncertainty, rapidly evolving regulatory complexity, cyberthreats, and significant climate risk—all of which can impact their portfolios. CROs also need to establish their role in the uncharted territory of emerging technologies, including gen AI, and their exponential growth. The emphasis on nonfinancial risk management is thus gaining traction. And we

are witnessing more boards expecting measurable progress across these topics to better protect the insurer and, ultimately, their shareholders and customers.

In this article, we share what insurance industry CROs identify as critical issues facing their organizations, focusing on selected priorities. We analyze the steps leaders in the field have taken to mitigate these risks and discern strategies by category—whether public, private, or mutual insurers. We then sketch a pathway forward, identifying issues early on and implementing agile and resilient systems to keep insurers not only healthy but also thriving.

How insurance CROs are approaching today's risks

Insurance risk leaders have identified several issues facing the industry and point to the strategic options they are using to mitigate these growing concerns.

Capital management is becoming an even more strategic topic due to changes in the economic and regulatory environments

While the inflation spike is less of a concern this year than it was in 2022 and 2023, changes to macroeconomic conditions, regulatory requirements, accounting standards, and the competitive landscape have put significant pressure on insurers' capital positions and are pushing them to strategically rethink their optimal balance sheet composition.

For P&C companies, capacity continues to be the biggest challenge. Losses from increasingly frequent and severe catastrophes, emerging exposures, and new types of risk have produced a surge in demand for insurance coverage. As always, insurers must control costs and derisk through repricing and reinsurance. In addition, sourcing alternative capital continues to play a meaningful role. The insurance-linked

¹ McKinsey's 2023 insurance risk and resilience benchmark.

securities (ILS) market grew by more than 20 percent year to year from 2022 to 2023. Catastrophe bonds alone hit an all-time high in the first two quarters of 2024.² Although ILS returns have been fluctuating, there are still investors willing to both look for assets that diversify their portfolios and seek attractive returns. New business models, such as public–private partnerships, present new opportunities for different capital participation models.

For life and annuity carriers, different ownership types drive different priorities. Under pressure from investors, public companies are shifting their focus toward capital-light businesses, utilizing reinsurance and other levers to optimize capital position and returns. Private-capital-backed carriers pay close attention to ownership structure and regulatory treatment based on locations that allow them to keep the growth momentum and take appropriate investment risk under specific capital regimes. Mutual companies are generally willing to accept lower returns, but they face the same pressure of having enough capital to back their policies and staying competitive and resilient under multiple shocks and market conditions.

To build resilience, carriers need to upgrade their stress-testing capabilities. While scenario planning is top of mind for carriers, applying the scenarios vary widely. In our industry benchmark, a third of insurers reported using no more than ten scenarios for risk appetite and capital requirement determination. Yet, another third reported using up to 250. In best practice, insurers are combining scenario simulation and “reverse stress testing” techniques³ to design and run a large number—as many as 10,000—of internally consistent macroeconomic scenarios and analyze a suite of financial measures at a granular level. By identifying potential early-warning indicators, those insurers are able to analyze the impact of management actions, create transparency on the assessment, and lead to a prioritized set of decisions.

Over time, capital management for CROs will continue to evolve from a compliance and risk play to a value creation play. This could mean moving from focusing on solvency ratio and excess capital to improving transparency on capital generation and uses of capital across business units and even products. The aim is to achieve an economic return on capital given the cost of capital for the insurer while maintaining a healthy level of excess capital. This shift would require the risk function to navigate complex (and sometimes multiple) capital frameworks, establish transparency on capital positions and uses (with possible capital reallocation across units, which is always a sensitive topic for the top team), enhance risk/return measures, and refine governance for decision making.

Gen AI at scale is expected to become table stakes for carriers; building a robust, risk-proof maintenance-at-scale model supported by the right talent will be critical

At our industry roundtable, technology, advanced analytics, and gen AI topped the list of concerns for insurance CROs. The emergence of gen AI has drawn considerable interest in the insurance world, as it does in banking, since it is viewed as both a disrupting force to the traditional business model and a powerful tool in the arsenal of underwriters, claims managers, and distribution leaders. Some insurers are considering its potential to transform distribution across life and P&C lines for both individual and commercial clients. The technology can help insurers understand the in-depth risk profiles of clients and produce much more tailored insurance contracts that suit their needs.

In a sector still defined by a high degree of manual processes and legacy systems, we expect a 10 to 30 percent increase in productivity across the risk and compliance function in insurance by deploying gen AI. Gen AI can enhance decision making by businesses by summarizing sets of documentation, improving the quality of policy information, and automating data extraction and operations.

² With nearly \$50 billion in catastrophe bonds and insurance-linked-securities risk capital outstanding as of May 2024, according to Artemis data.

³ As a complement to the more traditional approaches consisting of using deterministic scenarios to stress test a given portfolio, reverse stress testing to determine what multivariate scenarios would seriously impact the firm by generating tens of thousands of scenarios and quantifying interdependencies for less commonly understood scenarios as well.

A key opportunity presented by gen AI lies in addressing unstructured data. Despite strategic investments in analytics, carriers are acknowledging that data quality remains a core challenge for many of them. More than one-third of carriers in our benchmark indicated limited accuracy in maintaining a single source of truth for data.

At the same time, gen AI is also a risk that CROs and their teams will need to learn to manage in the second line of defense. The technology can present problems such as impaired fairness, intellectual property and privacy concerns, and security threats. As gen AI maturity evolves, the shortcomings of first-generation tools will be gradually addressed, especially privacy and fairness considerations.

Given gen AI's relatively novel risk profile and extremely rapid pace of development, carriers need to adapt their approach to fully integrate a transparent, responsible use of AI. In practical terms, this means establishing responsible gen AI principles and ethical guardrails, such as always having a human in the loop or restricting the use of gen AI for recruitment. Insurers must also establish risk ownership for each AI use case to ensure robust governance of AI implementation

and conduct regular risk assessments to analyze emerging gen AI risk trends. Making sure the risk and compliance, as well as legal, functions are integrated early on in the development and use of these new models is key.

The industry is also facing difficulties finding the right talent to address data and technology risk management. Nearly 60 percent of respondents in our benchmark reported that data and technology risk has been the most challenging area for attracting talent. This shortage of skilled personnel in the industry poses a hindrance to fully capitalizing on the opportunity of advanced analytics and gen AI. In our experience, companies must train the teams they have but be clear about the gen-AI-specific skills they need.

We offer one more consideration. Managing the potential risks of a dozen independent gen AI models in limited use (that is, proofs of concept), which is where most of the industry is today, is one thing. But having to maintain and manage risks with hundreds of gen AI models connected with one another across the organization and hundreds or thousands of external vendors will be a daunting proposition. Many insurers are not ready for it yet; it is a capability that needs to be built.

Given gen AI's relatively novel risk profile and extremely rapid pace of development, carriers need to adapt their approach to fully integrate a transparent, responsible use of AI.

Advanced climate risk management capabilities are becoming critical competitive differentiators

When adequately priced, insurance plays an important market-signal role regarding the inherent risks being insured. The rapidly evolving climate risk landscape—events such as wildfires, extreme heat, massive flooding, convective storms, and hurricanes—and the resulting tension between conditions of insurability and insurance affordability becomes more central for P&C carriers.

From 1980 to 2010, the United States faced an average of five severe natural catastrophic events (having an inflation-adjusted \$1 billion in damages or more) annually. Between 2011 and 2022, that number had tripled to an average of 15 per year, according to data collected by the US National Oceanic and Atmospheric Administration. Twenty-eight such events occurred in 2023. Insurance plays a critical role in helping insured disaster victims and affected areas recover faster. The weight of these mounting claims is pressuring underwriting profitability, reserve adequacy, and ultimately, the bottom lines of these P&C carriers. Their reinsurers have also often increased the retention (the level at which they will start reinsuring), leaving many insurers with retaining a more significant portion of the losses, especially for midsize events. All of this combined is forcing even the most sophisticated market leaders to fundamentally restructure their models, increase premiums, and shrink their exposure in certain areas, or even stop providing coverage altogether as several of them have recently done in California and Florida. At the same time, the nonadmitted property market in the United States is growing 20 percent annually, as customers are increasingly forced to pursue higher-cost, nonstandard property coverage.

With mounting natural catastrophes and scientific forecasts for a continued upward trend, investors and regulators are increasingly demanding that insurers better understand their climate risk exposures and be ready for nonlinear, abrupt changes in climate patterns. For carriers with significant commercial or personal-property

positions, investments in advanced climate analytics are becoming required capabilities, especially in combination with access to third-party data.

Life carriers are not immune to the climate risk conundrum. As large institutional investors, insurers are working to understand the impact of climate risk on their investment portfolios and liabilities. This is a result of recent climate risk disclosure rules, including those most recently adopted by the US Securities and Exchange Commission (SEC). On the asset side, transition risk, where changing economic conditions, market, and regulatory risks arise from the transition to a low-carbon economy, and physical risk, can fundamentally shift expected long-term returns in specific industries and asset classes.

The climate crisis is also influencing liabilities, affecting the longevity and health of policyholders. As shifting weather patterns and environmental factors impact public health, life carriers are considering the long-term effects on mortality rates, medical costs, and overall portfolio risk exposure. Carriers now face the complex challenge of factoring climate-induced health vulnerabilities into their actuarial models.

Overall, 60 percent of carriers in our latest industry benchmark reported accelerating efforts on climate risk management. The next generation of analytical capabilities is needed for insurers to integrate climate risk into organizational strategy. However, most insurers recognize that there is significant room for their climate analytical capabilities to mature: only one out of five carriers reported that they are able to quantify climate risks to the extent they would like to or have developed a forward-looking climate strategy to address climate risk exposure holistically for the organization. Boards are also getting heavily involved in the topic, with about half of carriers in our benchmark reporting having board oversight for climate risk, such as a sustainability committee. More frequent disasters, combined with new regulations, will only reinforce this trend.

Managing cyber risk is becoming a strategic priority for the second line, drawing significant investment and requiring strict prioritization

Insurers are also facing increased cyber risk exposure, as threats increase in sophistication and frequency. Insurers have access to large amounts of sensitive data that need protection. Among them are health and medical records, lists of insured items and properties, and wealth and assets under management. Even sophisticated, large carriers with significant investments in cybersecurity are not immune to such threats, with CrowdStrike reporting⁴ a 75 percent increase in cloud environment intrusions and Verizon reporting⁵ a 180 percent increase in breaches resulting from vulnerability exploitation. In addition, new cyberthreats are emerging, especially in connection with gen AI, and costs of cyberattacks are on the rise because of increasing fines, business losses, and remediation costs and often have significant reputational impact as well.

In this environment, cybersecurity is not only mandated by regulation; it is a core business requirement. Consumers and business partners are demanding that carriers put in place robust cybersecurity practices. At the same time, we see greater reporting requirements due to increased scrutiny from a variety of stakeholders, including the SEC's cybersecurity requirements. All major insurers have elevated cyber risk to the board level, with 50 percent of carriers discussing it quarterly.

Third-party cyber risk management, in particular, faces increased attention today. Carriers are called to examine who the core third parties are, and what their cyber risk levels are. For instance, do they process critical data or run a critical business process? Additionally, investors and regulators want to know if the carrier has additional concentration risk, and what a third party's software "bill of materials" is, such as a list of components that make up software components.

Carriers are expected to stay up to date with the latest developments in cyber technology and services, improving the organization's cybersecurity

posture while also reducing spending. Many of them use so-called zero trust architecture that shifts their cyber operating model to require strict identity verification. The majority of insurance CROs we work with take a proactive stance in monitoring and mitigating cyber risk in conjunction with the chief information security officer (CISO). However, about half of the carriers in our benchmark acknowledge that cyber expertise in the risk and compliance function is relatively new, as they are now building their cyber capabilities to oversee their CISO function. Investing in targeted capabilities that are truly second line and do not repeat what the first line is already doing will be accretive.

The key to success for carriers in the second line of defense—that is, efficient and effective oversight—is conducting targeted reviews based on cyber risk scenarios and on triggers for risk threats that are based on "cyber risk appetite." To address resource constraints, the risk team should understand key risks facing the carrier, credibly challenge internal policies, procedures, objectives, and performance, and provide the board and executive team with an independent view of the first line's program, including its testing.

Putting it together: Four moves for navigating a changing risk scenario for insurers

The aforementioned risk areas are select priorities where becoming distinctive can enhance the competitiveness and resilience of the company. To thrive in an environment of economic volatility and operating uncertainty, carriers can focus on four moves:

1. ***Continue to make the risk function more efficient.*** Insurers today face increasing cost pressure, which is impacting budgets for risk management, too. Among insurers with more than \$10 billion in revenues in our self-reported benchmark, the mean size of the risk function was slightly more than seven full-time employees (FTEs) per 1,000 FTEs in the company. That number was lower for

⁴ 2024 Global Threat Report, CrowdStrike.

⁵ 2024 Data Breach Investigations Report, Verizon.

Find more content like this on the
McKinsey Insights App



Scan • Download • Personalize



compliance (three FTEs per 1,000 FTEs). This can be a pivotal time to step back and continue to improve efficiency of core processes and clarify roles and responsibilities for the first and second lines. Cost savings can then be captured by making selective investments in efficiency—analytics and automation are good examples—while reducing check-the-box exercises. And while carriers will need to balance efficiency and effectiveness of their risk and compliance functions, they must consider a long-term perspective and make sure to keep residual risks under control.

2. **Build proper identification capabilities for emerging risks.** When executives across the organization have a clear and timely view of what key risks have already manifested or are currently emerging, the organization is able to navigate volatility and uncertainty most effectively. Those risks are not siloed either, and equipping the insurers with a better understanding of their interdependencies is important. This requires having in place data-enabled risk identification capabilities and flexible tech infrastructure to collect, aggregate, and monitor risk with timely data and to link it to a transparency dashboard on risk appetite. Advanced scenario planning can help here as well.
3. **Shift risk and compliance “to the left.”** Ensuring the risk and compliance functions are at the business decision table early on is key. This is especially important for emerging risks. This is a shift away from being the final reviewers and approvers—the “right” of the decision-making process—to the left of the process, where they are an integral part of the development of new products, policies or changes. This shift to the left fosters a healthy risk-based decision-making culture

and, ultimately, faster execution within a given risk appetite. Leaders in these functions need to be agile and ready to innovate as a business partner, not just a pure control function.

4. **Enhance strategic agility and resilience.** In the face of uncertain economic conditions and evolving industry landscapes, insurers should prioritize enhancing their strategic agility and resilience. This involves not only preparing for known risks but also building the capacity to adapt swiftly to unforeseen challenges. Implementing flexible strategies and agile operational frameworks can empower organizations to respond dynamically to changes, whether they arise from market shifts, technological advancements, or regulatory updates.

Today, insurance industry CROs are facing multiple demands from both relatively well-known and new risks. Industry leaders are resisting short-term actions and are instead focusing on the financial and nonfinancial risks that matter most, making selective investments in capabilities such as advanced analytics and gen AI. CROs, working with the CEO, the full executive team, as well as the board’s audit and risk committees, are also building proper emerging-risk identification capabilities, fostering a culture of innovation, enhancing strategic agility and resilience, and prioritizing the management of technology. All of this is in service of protecting the firm, its customers, its employees, and in the end, its shareholders.

While risks are ultimately owned by the first line of defense, the CROs—whether they have been in the seat for long or are new to the role—are playing a more strategic role than they did just five years ago. We expect this trend to accelerate.

Erwann Michel-Kerjan is a partner in McKinsey’s Philadelphia office, and **Lorenzo Serino** is a partner in the New York office.

The authors wish to thank Dimitris Paterakis, Justin Greis, Liz Grennan, and Ying Zhao for their contributions to this article.

Designed by McKinsey Global Publishing
Copyright © 2024 McKinsey & Company. All rights reserved.