

Chief Risks Officers Dialogue Series



Risk Management, Reimagined: Outlook to 2035

WHITE PAPER
SEPTEMBER 2026



Contents

Executive summary	3
1 Why risk management must evolve	4
1.1 Traditional risk frameworks may not work well anymore	4
1.2 Risks are increasingly interconnected	5
1.3 Preparedness, not prediction, needs to be core in future risk management	7
1.4 Evolution beyond shared governance, risk and compliance roots	8
2 The evolving role of the CRO	9
2.1 Shape strategy instead of reviewing it	10
2.2 Generate risk intelligence and enable business velocity	11
2.3 Validate assumptions rather than only scoring risks	11
2.4 Build capabilities to adapt to, not just mitigate, disruption	12
2.5 Artificial intelligence to complement human intelligence, not substitute it	12
2.6 Business managers, not just risk managers	13
3 Building the risk-ready organization	14
3.1 Continuous sensing and early warning	14
3.2 Scenario planning and digital twins	15
3.3 Recognizing and integrating regional nuances	16
3.4 Balancing between AI and human intelligence	17
Conclusion: En route to 2035 – strategic considerations	20
Contributors	21
Endnotes	22

Disclaimer

This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

© 2026 World Economic Forum. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

Executive summary

Traditional enterprise risk management needs to pave the way for proactive, real-time risk monitoring and intelligence.

Today, organizations face a fundamentally different risk landscape from the one that shaped traditional **enterprise risk management (ERM)**. Geoeconomic fragmentation, technological disruption, cyber insecurity, climate volatility and societal polarization, among other risks, are interacting more deeply and materializing more rapidly than traditional frameworks were designed to manage. For example, cyber incidents can quickly trigger geopolitical tensions, while climate events can suddenly disrupt supply chains and contribute to social instability.

The challenge facing organizations today is how to adapt and make confident decisions in an environment where uncertainty has become structural rather than episodic, and risks are increasingly interconnected and nonlinear. Consultations with chief risk officers (CROs) point to a common thread: the role of risk management is undergoing a fundamental transformation. The survey on the future of risk management conducted for this paper reveals that 80% of CRO respondents believe risk management will be “somewhat to far more challenging” in 2035 compared to today. Historically, risk functions were designed to protect organizations by identifying risks, ensuring compliance and maintaining effective controls. Increasingly, they are becoming strategic capabilities embedded within decision-making itself. In future, risk teams will need to help organizations interpret uncertainty, challenge assumptions, evaluate trade-offs and strengthen long-term resilience. Only 10% of CROs describe their organization

as “very prepared to respond to risks that can’t be modelled with historical data”.

The paper identifies four shifts that are likely to define the next generation of risk management:

1. Organizations will move from **prediction to preparedness**. Resilience will depend less on accurately predicting individual events and more on developing the governance, capabilities and decision processes required to respond effectively.
2. Risk management will evolve from **compliance to strategic enablement**. The future CRO will increasingly participate in the early stages of strategic decisions rather than reviewing them after the fact.
3. Organizations will transition from **periodic reviews to continuous risk monitoring and intelligence**. AI-enabled sensing, real-time monitoring and integrated risk intelligence will replace static reporting cycles.
4. **Artificial intelligence (AI)** will complement human intelligence in the three above areas. AI will automate monitoring, aggregation, anomaly detection and simulation. Advances in digital twins, AI-driven simulation and dynamic scenario planning will allow organizations to stress-test decisions, explore multiple plausible futures and build resilience before crises occur.

1

Why risk management must evolve

New, emerging and interconnected risks will make the future of risk management far more challenging than it is today.

1.1 Traditional risk frameworks may not work well anymore

Modern enterprise risk management (ERM) emerged during a period characterized by increasing globalization, relatively stable geopolitical relationships and growing confidence in data-driven decision-making. Risk frameworks were designed to identify threats, estimate their likelihood and impact, and implement controls to reduce exposure. These approaches remain valuable and continue to provide important insights for many categories of risk.

However, the assumptions underpinning traditional risk management are increasingly being challenged. Many organizations continue to rely heavily on

historical data, probability assessments and periodic risk reviews. Yet future disruptions may not resemble those of the past. Emerging technologies, shifting geopolitical dynamics and environmental changes, among other drivers, are creating risks with limited historical precedent that cannot be easily quantified using conventional methodologies.¹

Chief risk officers (CROs) emphasize that, while historical models remain useful for understanding familiar risks, they become less reliable when organizations confront new and emerging threats.

“

Banking risk management has traditionally relied on observed default rates, loss histories and data on economic downturns. However, emerging risks such as AI-enabled cyber threats (including attacks on real-time payment systems) and geoeconomic fragmentation may not follow patterns inferred from the past. Future crises may not resemble prior crises, and risk functions that rely too heavily on historical analogues may fail to detect vulnerabilities until they have already materialized.

Damian Vogel, Chief Risk Officer, UBS

“

The speed of change and interconnectedness of risks make it important to treat uncertainty as a baseline; we have to let go of the fundamental assumption that markets are predictable and mean-reverting. Volatility, today and in the future, is structural, rather than episodic.

Qiniso Mthembu, Group Chief Risk Officer, Johannesburg Stock Exchange (JSE)

“

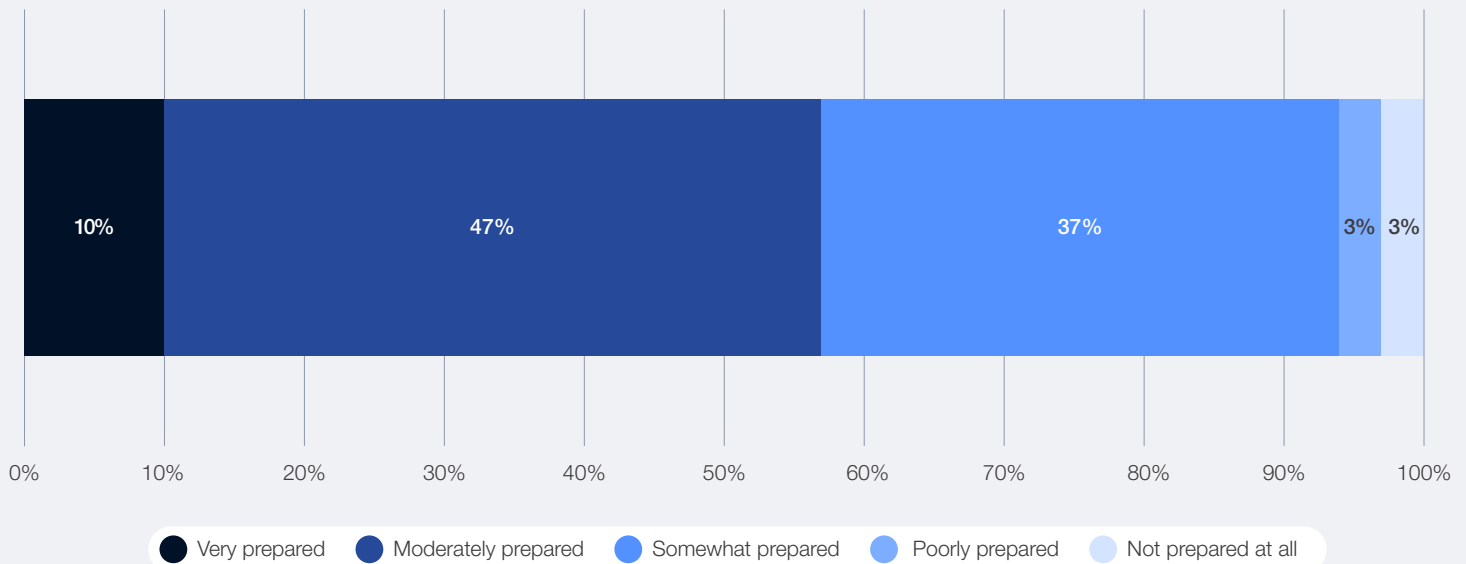
Organizations are increasingly confronting the challenge of speed, in addition to a range of other complexities. For example, geopolitical developments, regulatory changes, cyber incidents and technology disruptions can materialize within hours rather than over months or years. The future of risk management will be shaped not only by the nature of risks themselves but also by their velocity.

Monica Morata Videira, Head, Enterprise Risk Management, SAP

Risk assessments conducted annually or even quarterly may struggle to capture rapidly evolving developments. Information flows are becoming faster, and stakeholder expectations are changing more quickly. As a result, risk management must provide real-time insights rather than periodic evaluations.

A survey of members of the World Economic Forum's CRO Community was conducted to gauge sentiment on the future of risk management. This survey shows that only 10% of CROs describe their organization as "very prepared to respond to risks that can't be modelled with historical data". (Figure 1). However, 80% believe that risk management will be somewhat to far more challenging in 2035 compared to today.

FIGURE 1 Question: How prepared is your organization to respond to risks that cannot be modelled using historical data?



Source: World Economic Forum. (2026). Survey of CRO Community.

1.2 Risks are increasingly interconnected

The growing interconnectedness of risks is a major challenge. Organizations have traditionally categorized risks into discrete areas such as operational, financial, geopolitical, technological or environmental risks. While these classifications remain useful, they increasingly fail to capture the complex interactions between the different risk categories. Recent years have demonstrated how quickly disruptions can cascade across systems. Risks do not occur in isolation but reinforce and amplify one another.²

Yet, the current environment is not characterized simply by the simultaneous occurrence of multiple crises. Rather, it involves situations in which distinct disruptions (such as geopolitical tensions, cyber incidents, climate shocks, supply-chain disruptions, technological change and economic instability) interact with and reinforce one another, creating cascading effects that are difficult to anticipate or manage through traditional approaches.

When this happens, the consequences of one disruption often alter the likelihood, severity or trajectory of another. A cyberattack may disrupt critical infrastructure, triggering supply chain bottlenecks that amplify inflationary pressures and provoke political responses.³ A climate-related disaster may affect energy systems, commodity markets and migration patterns simultaneously.⁴ What makes these situations particularly challenging is that organizations are not responding to a single event, but to a dynamic system of interacting shocks.

This represents a fundamental departure from the assumptions that underpin many conventional risk management frameworks. Traditional approaches often assess risks individually. However, the most significant threats may emerge not from individual risks themselves, but from the interactions between them. As a result, organizations can find themselves exposed to vulnerabilities that are difficult to identify



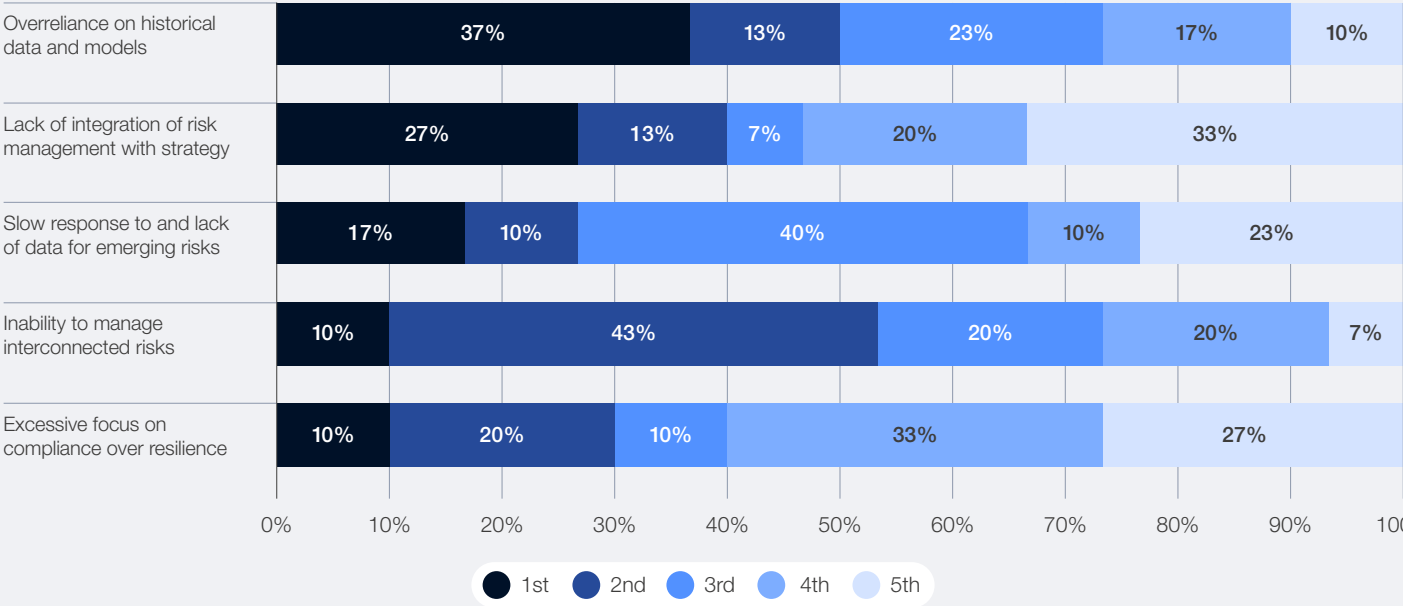
through segregated risk assessments or static risk registers.⁵

The CROs reiterated that future risk management must focus less on individual risk categories and more on understanding interdependencies. Organizations need to understand how vulnerabilities in one area may affect others and

how external disruptions can propagate through increasingly interconnected systems.

More than 70% of CROs surveyed indicated that the inability to manage interconnected risks and overreliance on historical data and models both feature in the top three limitations of current risk management approaches (Figure 2).

FIGURE 2 Question: What is the biggest limitation of current risk management approaches? Ranked 1 (highest) – 5 (lowest)



Source: World Economic Forum. (2026). Survey of CRO Community.

1.3 Preparedness, not prediction, needs to be core in future risk management

As uncertainty increases due to the emergence of new and interconnected risks, preparedness becomes more important than prediction. This does not mean organizations should abandon

forecasting or quantitative modelling. Rather, these tools should be complemented by capabilities that enable organizations to respond effectively when assumptions fail and unexpected events occur.



Future risk management will depend less on predicting crises and more on ensuring that organizations are prepared to respond effectively when crises occur. Organizational resilience is like aviation safety; pilots cannot anticipate every possible emergency, but they are trained to respond through well-defined procedures, governance structures and decision protocols. Similarly, organizations cannot predict every disruption. What they can do is build the capabilities, processes and decision-making disciplines required to adapt rapidly to unexpected events.

Damian Vogel, Chief Risk Officer, UBS



1.4 Evolution beyond shared governance, risk and compliance roots

For much of the past three decades, risk and compliance have shared a common institutional history, frequently organized within a single governance, risk and compliance (GRC) framework. Compliance was the function that matured first, driven by regulation, enforcement and clearly defined obligations. Risk management, meanwhile, remained closely tied to risk registers, controls testing and assurance activities. Those foundations remain essential. What has changed is the relative weight of the two disciplines. In an environment where uncertainty is structural rather than episodic, risk management has become one of the decisive capabilities for a company's long-term success – not an extension of compliance, but a strategic function in its own right.

However, many of the risks shaping the next decade differ fundamentally from those that traditional frameworks were designed to address. Geopolitical fragmentation, AI-driven cyber threats and urgent supply chain reconfigurations are examples of risks that cannot be managed solely through controls, compliance processes or periodic assessments. They involve strategic choices, uncertain futures and complex trade-offs. As a result, organizations increasingly require risk functions that do more than monitor exposures – that help leadership teams navigate uncertainty before decisions are made.

Going beyond compliance and control does not mean abandoning oversight responsibilities. Rather, it means expanding the role of risk management from protecting value to helping create and sustain it. In practice, this involves integrating risk perspectives into strategic planning, capital allocation, technology investments, market entry decisions and business transformation initiatives.

Recent market research supports these views. Several studies argue that risk management is moving from a defensive capability towards a source of strategic value, with leading organizations embedding risk considerations directly into transformation and innovation agendas.^{6,7}

Taken together, these developments point to a broader shift in mindset. Historically, risk management has often been viewed as a mechanism for reducing uncertainty and preventing adverse outcomes. Increasingly, however, organizations are recognizing that uncertainty often cannot be eliminated and that many strategic opportunities emerge precisely because uncertainty exists. The future role of risk management is therefore not simply to help organisations avoid risk, but also to help them navigate uncertainty with greater confidence, resilience and strategic clarity.



Risk management is shifting from a rather compliance-focused function towards a strategic business enabler, driving value creation, growth and resilience.

Lisa Bechtold, Chief Risk Officer, Nestlé



Risk management can no longer remain confined within traditional GRC structures. While compliance functions often focus on short-term obligations and mandatory requirements, future risk management must adopt a longer-term, more strategic perspective.

Torben Oeder, Head, Group Risk Management, Volkswagen



The future role of ERM is not simply to identify risks or coordinate reporting, but to bring together functions that often operate independently – from compliance and cybersecurity to business continuity and strategy.

Diane Doering, Global Head, Enterprise Risk Management, Takeda

2

The evolving role of the CRO

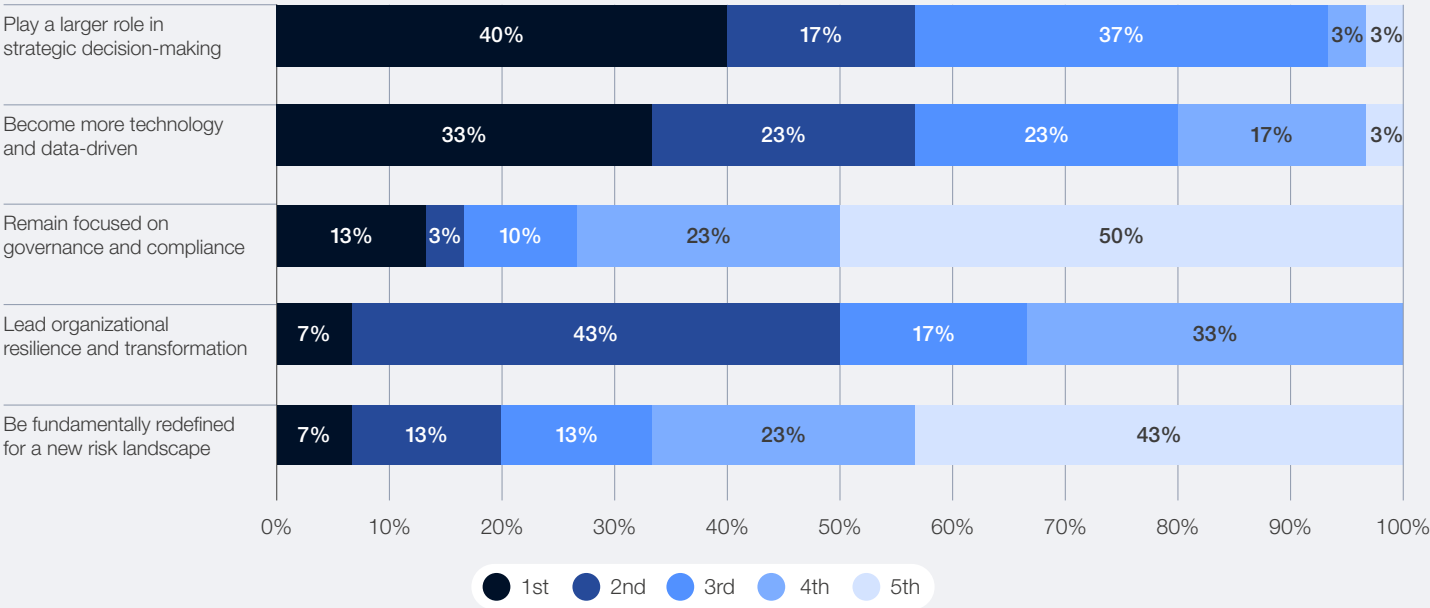
The 2035 CRO will build organizational adaptability to risks while being closely involved with strategy and business decision-making.

The role of the CRO is evolving alongside these changes. Traditionally, CROs were positioned as guardians of organizational discipline, responsible for monitoring exposures and ensuring appropriate controls. Increasingly, however, organizations are expecting CROs to contribute directly to strategic discussions and long-term planning. In the CRO

survey, 40% indicated that playing a larger role in strategic decision-making would be the most important evolution in future risk management practices, while 33% believed that becoming technology- and data-driven would be the most important ask of their future job description (Figure 3).

FIGURE 3

Question: How do you expect the role of the CRO to evolve over the next 5-10 years?
Ranked 1 (highest) – 5 (lowest)



Source: World Economic Forum. (2026). Survey of CRO Community.



2.1 Shape strategy instead of reviewing it

As future CROs increasingly participate in strategy formulation itself, their role will be to challenge assumptions, assess alternative pathways and identify vulnerabilities before major decisions are finalized.

80% of CROs surveyed believe that embedding risk into strategic decision-making is one of the top three capabilities critical for the future of risk management (Figure 4).



Risk leaders should be involved in strategic discussions from the outset rather than being consulted only during mitigation phases.

Natasha Fields, Chief Risk Officer, World Trade Organization (WTO)

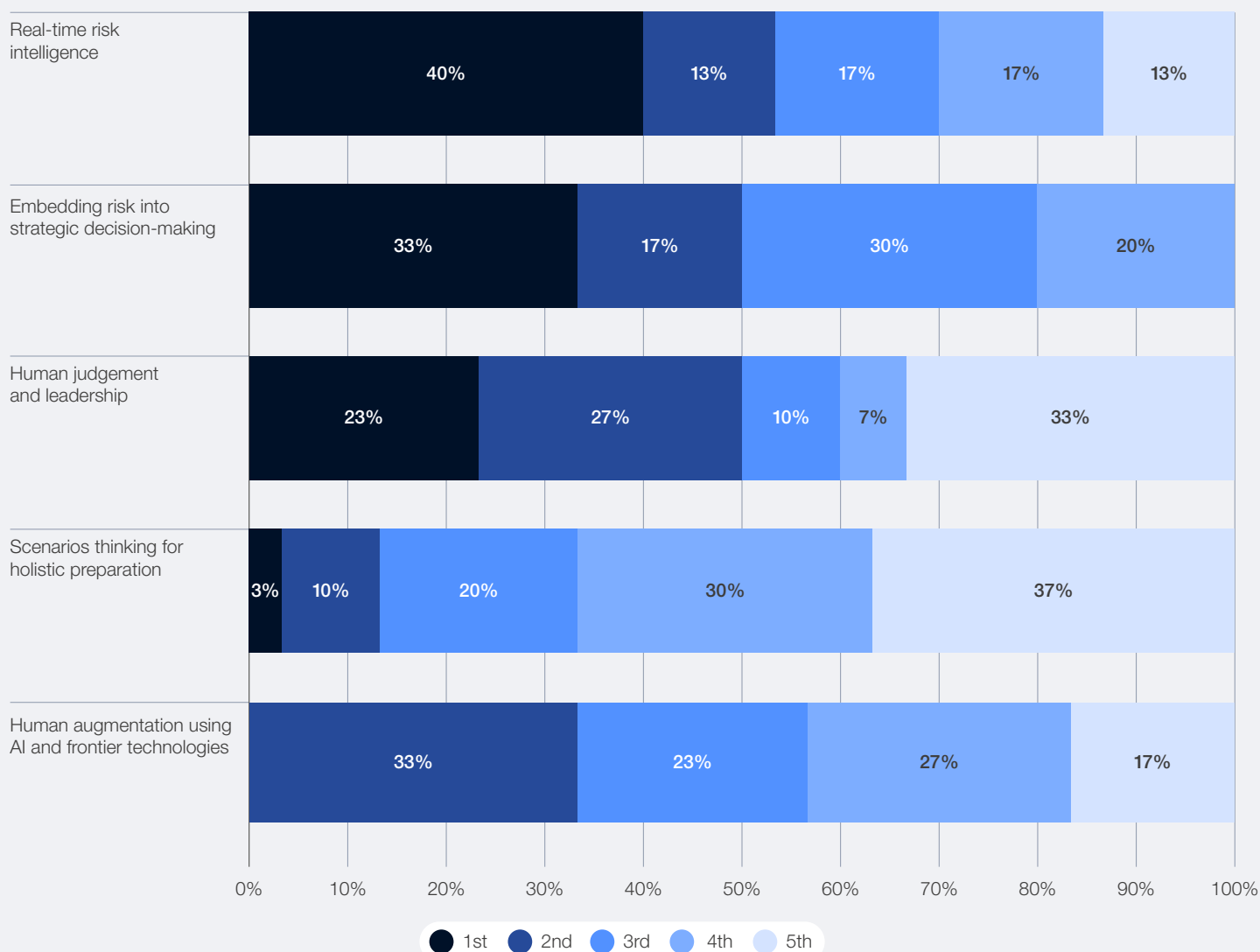


Risk management must move closer to the Chief Executive Officer and strategy functions if it is to create business value rather than primarily satisfy audit and governance requirements.

Torben Oeder, Head, Group Risk Management, Volkswagen

FIGURE 4

**Question: Which capability will be most critical for the future of risk management?
Ranked 1 (highest) – 5 (lowest)**



Source: World Economic Forum. (2026). Survey of CRO Community.



2.2 Generate risk intelligence and enable business velocity

In environments characterized by continuous change, organizations are increasingly moving towards dynamic approaches that emphasize continuous sensing, real-time monitoring and forward-looking analysis. Future CROs will be expected to provide continuous risk intelligence: identifying weak signals, interpreting emerging

developments and helping leadership teams understand how external shifts could affect strategic priorities. This implies that the role of the CRO will shift from cataloguing risks to generating actionable insights. This shift from a reactive to a proactive role will help the CRO become an enabler of business velocity.



Future CROs may increasingly be evaluated not only on their ability to protect the organization, but also on how effectively they enable it to move. As product development cycles shorten and competitive advantage increasingly depends on speed to market, risk functions will face growing expectations to accelerate decision-making rather than delay it. This represents a fundamental shift in performance expectations: future CROs may be measured using metrics such as decision turnaround time, client outcomes and organizational efficiency alongside more traditional measures of risk management effectiveness.

Paul Gibson, Partner, Heidrick & Struggles

2.3 Validate assumptions rather than only scoring risks

Traditional risk frameworks focus on estimating the probability and impact of identified risks. However, several surveyed CROs argued that future resilience

will depend less on precise risk scoring and more on understanding which assumptions underpin organizational strategies.



Novartis has introduced assumption auditing, systematically identifying and stress-testing the assumptions that support strategic decisions. The CRO's role is not only to ask 'What are the risks?' but also to investigate 'What must remain true for this strategy to succeed?'

Barbara Badoino, Head, Corporate Ethics, Risk and Compliance, Novartis

2.4 Build capabilities to adapt to, not just mitigate, disruption

Historically, risk management has often been evaluated according to its ability to mitigate losses or avoid adverse outcomes. In a world characterized by multiple rapidly evolving and interconnected crises, preventing every disruption is no longer a realistic objective. Future CROs must be

capable of communicating uncertainty to decision-makers and translating complex risk information into actionable insights. They will increasingly focus on building organizational adaptability – strengthening governance, decision-making processes, crisis response capabilities and organizational resilience.

2.5 Artificial intelligence to complement human intelligence, not substitute it

Artificial intelligence (AI) will increasingly augment risk management by identifying patterns, monitoring exposures and generating predictive insights. However, CROs emphasized that accountability and judgement will remain human responsibilities.

The future CRO will act as an orchestrator between machine intelligence and executive decision-making. Their role will not be to compete with AI systems but to interpret outputs, provide context, challenge conclusions and ensure that decisions remain aligned with organizational objectives and values.



While AI may significantly enhance analytical capabilities, humans will continue to play a critical role in connecting disparate signals, evaluating ambiguity and taking responsibility for strategic decisions.

Lisa Bechtold, Chief Risk Officer, Nestlé



2.6 Business managers, not just risk managers

“ The future CRO must contribute to commercial judgement along with risk perspectives. Increasingly, risk leaders are expected to participate at the inception of investment decisions, acquisitions and strategic initiatives, evaluating the viability of opportunities under different risk scenarios. This represents a significant shift from traditional models in which risk teams reviewed decisions after they had been developed. Future CROs will therefore need to understand business models, market dynamics and investment decisions as deeply as they understand risk frameworks.

Bhaskar Mehta, Chief Risk Officer, GFH Financial Group

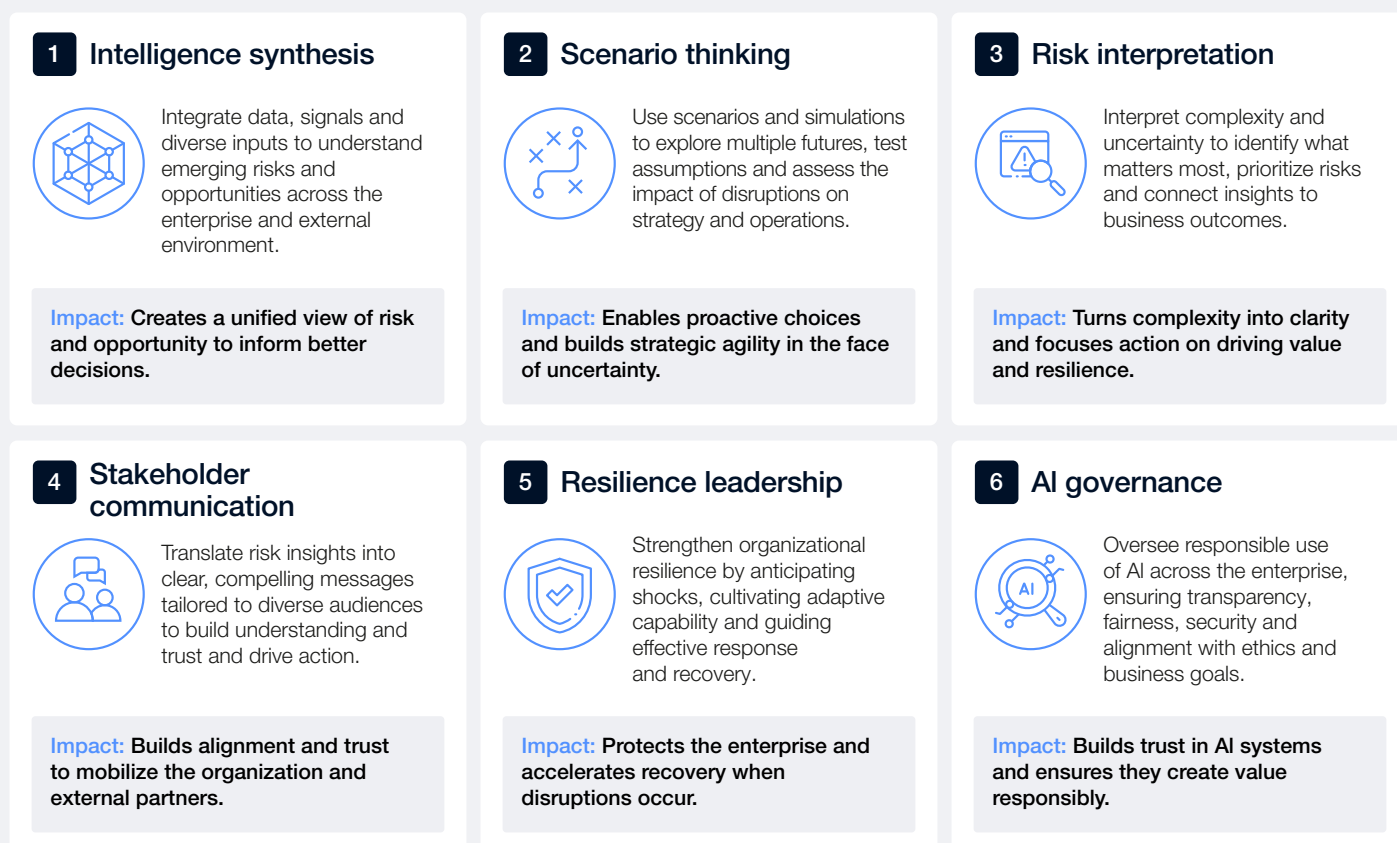
“ It's crucial to visualize a broader evolution in which the future CRO could become a trusted adviser embedded within a business decision-making process.

Monica Morata Videira, Head, Enterprise Risk Management, SAP

So, what will a day at work look like for a CRO a decade from now? It could start with examining a dynamic intelligence platform that continuously monitors geopolitical developments, climate indicators, cyber threats, regulatory changes and operational performance, among other indicators. Even if no major crisis occurs, it is important to review the various assumptions underpinning the organization's strategy. Each day could provide a

new complex situation – regulations could emerge in a key market, an extreme weather event could be unfolding in a major production region, or geoeconomic tensions could be affecting critical supply chains. The organization's systems detect these developments automatically. The role of the CRO is to understand and interpret what they mean. Figure 5 illustrates the key skills that the CRO of 2035 must possess.

FIGURE 5 2035 CRO core skillsets



Building the risk-ready organization

A risk-ready organization will use AI for sensing, monitoring and anomaly detection while humans will retain interpretation, judgement and accountability.

Building a risk-ready organization requires more than strengthening the risk function alone. It involves new capabilities that enable the organization to continuously sense change, rehearse future disruptions, incorporate regional

context and combine AI with human judgement. The following capabilities illustrate how leading organizations are beginning to redesign risk management for this new operating environment.

3.1 Continuous sensing and early warning

One of the most significant shifts shaping the future of risk management is the move from periodic assessments towards continuous sensing. Traditional approaches rely on annual reviews, quarterly updates and retrospective reporting. As risk environments become more dynamic, organizations are increasingly complementing these processes with capabilities that continuously monitor emerging risks and changing conditions.⁸

Advances in AI, automation and data analytics now allow organizations to track developments across supply chains, markets, regulation, cybersecurity, geopolitics and public sentiment in near real time. Rather than waiting for formal assessment cycles, risk teams can identify anomalies, detect

weak signals and escalate emerging concerns as conditions evolve.⁹ For example, in leading financial services companies, AI-enhanced risk models incorporate real-time economic indicators, market signals and external news flows into forecasting and stress-testing processes.

Importantly, continuous sensing extends beyond internal operations. Emerging approaches integrate external intelligence, including geopolitical developments, regulatory changes, labour disputes and reputational signals. AI-powered tools can process large volumes of information and highlight developments that may have implications for strategy, operations or resilience.¹⁰



Predictive analytics and AI-enabled early warning systems are highly relevant as they connect data across supply chains, climate indicators and operational performance.

Lisa Bechtold, Chief Risk Officer, Nestlé



A transition is occurring from annual risk cycles towards continuous monitoring of signals and assumptions.

Barbara Badoino, Head, Corporate Ethics, Risk and Compliance, Novartis



The future of risk management lies less in maintaining risk registers and more in generating risk intelligence that helps decision-makers interpret uncertainty in real time.

Natasha Fields, Chief Risk Officer, World Trade Organization (WTO)



There will be a marked shift from pull-based risk management, where risks are identified through periodic assessments or requests, towards push-based models in which emerging risks are continuously surfaced and escalated as conditions change.

Monica Morata Videira, Head, Enterprise Risk Management, SAP

Indeed, 70% of the CROs who responded to the survey believe that real-time risk intelligence is one of the top three capabilities critical for the future of risk management (Figure 4).



3.2 Scenario planning and digital twins

Historically, scenarios, tabletop exercises and stress tests have helped organizations explore potential disruptions and challenge assumptions. While valuable, these exercises are often static and limited in scope. As uncertainty becomes more difficult to quantify, organizations are increasingly looking beyond traditional scenario planning approaches.

The next generation of scenario planning is likely to be more dynamic, continuous and data-driven. Advances in digital twins and other simulation technologies are enabling organizations to move beyond a small number of predefined scenarios towards continuously evolving future environments. Rather than asking leadership teams to choose between three or four alternative futures, it is possible to generate and test thousands of combinations of geopolitical developments, regulatory shifts, climate events, technology disruptions and market changes.¹¹

One promising development is the emergence of digital risk twins – dynamic virtual representations

of an organization's risk landscape that combine real-time data, system dependencies, expert judgement and simulation capabilities. Unlike traditional risk models, which often assess risks individually, digital risk twins are designed to capture interactions between risks, reveal hidden vulnerabilities and simulate how disruptions may cascade across complex systems.¹²

The significance of these technologies lies not in predicting specific events. Rather, they allow organizations to safely and systematically experiment with uncertainty. Risk teams can test how different interventions perform under multiple conditions, explore the consequences of disrupted assumptions and identify vulnerabilities before they emerge in the real world. Research suggests that such simulations are particularly valuable for understanding nonlinear effects, cascading failures and second-order consequences that are often overlooked in conventional risk assessments.¹³

Several CROs validated the need to have cutting edge scenario planning in place.



Organizations increasingly have insufficient time to predict and prepare for risks sequentially. Instead, they must develop the capability to continuously evaluate how emerging developments could alter future operating conditions.

Natasha Fields, Chief Risk Officer, World Trade Organization (WTO)



Organizations should become more comfortable exploring uncertainty rather than attempting to eliminate it.

Barbara Badoino, Head, Corporate Ethics, Risk and Compliance, Novartis

Both the above perspectives point towards a future in which risk management focuses less on predicting specific events and more on continuously exploring how different futures could unfold.



It's crucial to integrate scenarios that simulate multiple threats simultaneously, such as cyber, geopolitical and market risks, to better prepare for cascading events and build effective early warning capabilities.

Qiniso Mthembu, Group Chief Risk Officer, Johannesburg Stock Exchange (JSE)

AI-enabled digital twins are already being used to support preparedness by allowing organizations to simulate, for example, responses to floods, infrastructure failures and other complex disruptions before they occur. Similar approaches are likely to increasingly be applied to supply chains, business models and geopolitical exposures.

The purpose of these capabilities is rehearsal. As risks become more interconnected and volatile, preparedness may depend less on forecasting specific events and more on continuously testing how organizations would respond if different futures emerged.

3.3 Recognizing and integrating regional nuances

Organizations need to develop risk capabilities that consider regional realities and experience.

Regional exposure shapes institutional capabilities and risk frameworks.



Different regions have different historic risk management experiences. Switzerland's long banking history has contributed to deep expertise in counterparty and credit risk management. Meanwhile, Japan's experience with the 1986–1991 asset bubbles and subsequent prolonged stagnation shaped sophisticated approaches to deflationary and balance-sheet risks.

Bhaskar Mehta, Chief Risk Officer, GFH Financial Group

Such geographic uniqueness in risk exposure creates distinct risk cultures – what becomes a priority in one location may be entirely absent from another's risk radar. This regional variation needs to be factored in when thinking about the risk universe. It should also influence the types of

expertise that risk management teams develop over time, with each regional risk team building depth in areas where they have direct exposure.

An example of an area that needs consideration is region-specific climate risk.



There is growing interdependence between AI and climate risk. As AI adoption accelerates, so will demand for data centre capacity and energy and cooling infrastructure. Future risk management will therefore need to consider not only the risks posed by AI, but also the environmental and infrastructure dependencies that underpin the AI ecosystem itself. Organizations operating in regions that are more pressed for energy resources, or where the impact of climate change is more strongly felt, need to be mindful of their AI energy and resource consumption.

Christos Christou, Chief Risk Officer (CRO), LuLu Financial Holdings



It is also important to note that regulatory landscapes differ widely across regions, and, as geoeconomic confrontation is likely to persist or

even deepen in the coming years, that regulatory divergence will increasingly need to be factored into risk management.



The challenges in balancing innovation with regulatory compliance are different in different markets. It is important to engage regulators early on in the innovation process and co-create and co-curate with them to demonstrate how future risk management practices will protect markets and maintain integrity.

Qiniso Mthembu, Group Chief Risk Officer, Johannesburg Stock Exchange (JSE)

3.4 Balancing between AI and human intelligence

AI is unlikely to replace risk managers. It is more likely to reshape how risk management work is divided between machines and humans. Across all the consultations with CROs, a consistent picture emerged: AI will increasingly assume responsibility for monitoring, aggregation and pattern recognition, while humans remain responsible for interpretation, judgement and accountability.

Several risk leaders argued that AI's greatest value lies in areas where large volumes of information must be processed continuously. Risk sensing, anomaly detection, cyber threat monitoring, third-party risk surveillance and regulatory scanning are all becoming increasingly data-intensive

activities. AI's ability to aggregate information, identify patterns and detect anomalies across large datasets in near real time will only get better in the next decade. For example, Mastercard's fraud systems analyse billions of transactions annually and generate risk scores in milliseconds.¹⁴ Similar approaches are increasingly being applied to cyber monitoring, operational resilience and third-party risk management.

AI is also likely to play an increasingly important role in connecting fragmented risk information. Organizations often maintain separate assessments for cybersecurity, privacy, compliance, operational resilience, climate and emerging technologies.



One of the most promising applications of AI lies in integrating perspectives and identifying blind spots, overlaps and interdependencies that individual teams may overlook. Rather than generating another layer of reporting, AI may increasingly serve as connective tissue across the enterprise.

Diane Doering, Global Head, Enterprise Risk Management, Takeda



AI has the potential to fundamentally change how risk organizations access information by centralizing regulatory requirements, internal policies, controls and organizational risk appetite into a single knowledge environment. Such an integration will enable the development of a more unified intelligence capability while significantly reducing duplication. Automation is likely to have its greatest impact on highly structured activities such as testing, financial crime monitoring and quality assurance. These processes have long been candidates for automation, with AI accelerating rather than initiating this transition.

Paul Gibson, Partner, Heidrick & Struggles

However, there are also aspects of risk management that are highly unlikely to be delegated to AI.

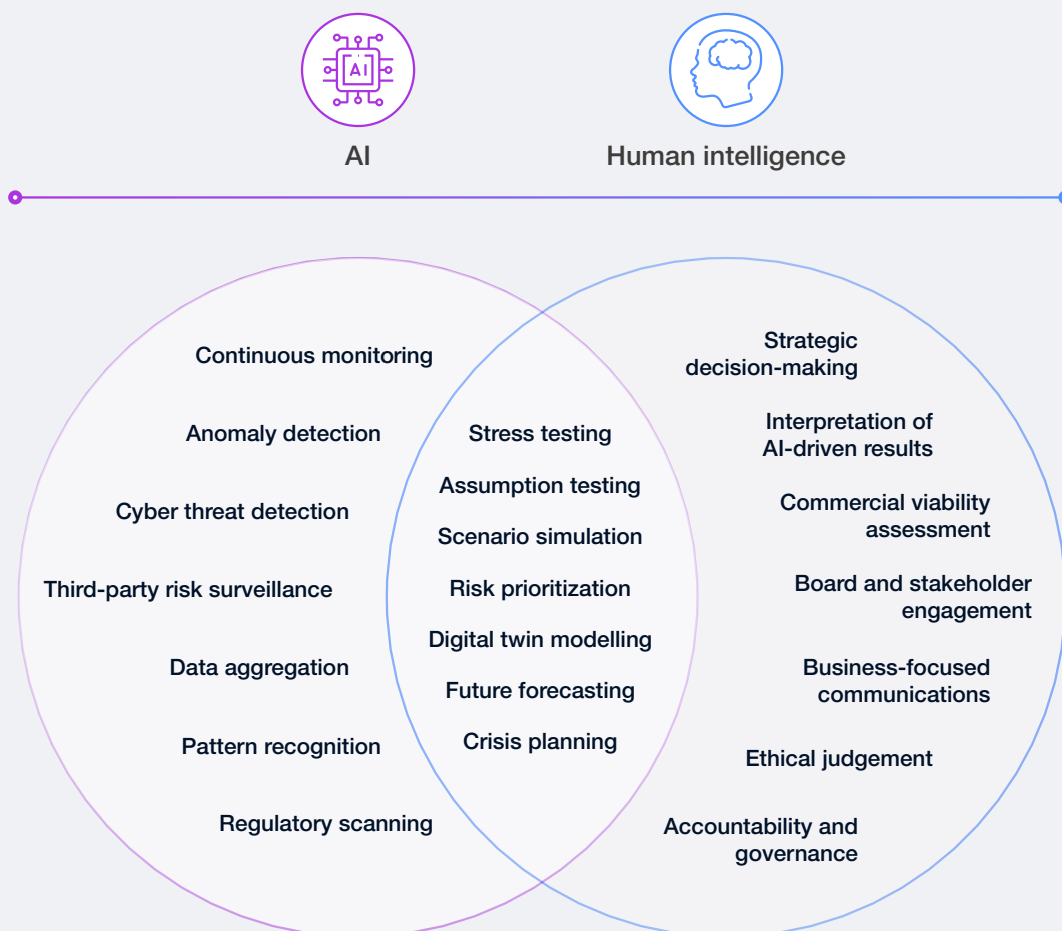


AI can generate insights and play a critical role in augmenting human decision-making, but humans remain responsible for providing context, interpreting results and ensuring that business decisions align with strategic objectives and organizational values.

Lisa Bechtold, Chief Risk Officer, Nestlé

- “ **While AI may identify risks, it cannot fully understand unique geographic contexts, commercial realities or ethical trade-offs.**
- Bhaskar Mehta, Chief Risk Officer, GFH Financial Group
- “ **Future risk leaders will increasingly serve as interpreters of AI-generated insights, helping executive teams distinguish meaningful signals from noise.**
- Torben Oeder, Head, Group Risk Management, Volkswagen
- There is also the less-discussed challenge of preserving human expertise in an increasingly automated environment. There are concerns about how future professionals will develop the skills needed to challenge AI-generated outputs if they become overly dependent on automated systems.
- “ **AI is most effective when applied to well-designed processes and high-quality data. Poor processes (with poor-quality data) do not become better when automated; they simply operate faster.**
- Monica Morata Videira, Head, Enterprise Risk Management, SAP
- The future of risk management is therefore unlikely to involve a simple trade-off between humans and machines. Instead, it will lead to a new division of labour. AI will increasingly perform the tasks that require scale, speed and continuous monitoring. Humans will continue to provide judgement, challenge assumptions, evaluate trade-offs and take accountability for decisions (Figure 6). As risk environments become more complex, the competitive advantage may come not from having more AI, but from knowing how to combine machine intelligence with human expertise most effectively.

FIGURE 6 **AI and human intelligence interaction**



Source: World Economic Forum.

Emerging technologies are changing the physical infrastructure on which organizations depend.



Advances in AI and quantum computing will require significantly greater compute capacity, data storage and energy infrastructure. These developments introduce new categories of risk that extend beyond software, including hardware resilience, energy availability, cooling capacity and environmental sustainability. In this context, the future of risk management must increasingly consider the resilience of the digital infrastructure that enables technological transformation.

Christos Christou, Chief Risk Officer, LuLu Financial Holdings



Conclusion: En route to 2035 – strategic considerations

For decades, ERM has helped organizations strengthen governance, improve transparency and protect against financial and operational losses. The CRO consultations conducted for this paper revealed that, while still necessary, this will no longer be sufficient for the next decade of risk management. The organizations that succeed over the coming decade will have to thrive in environments where disruption is continuous, risks interact across systems and strategic decisions increasingly need to be made without complete information. Across every consultation, regardless of geography or industry, one message was clear: the future CRO will become less of a risk controller and more of an interpreter of uncertainty.

AI, simulation environments and continuously connected data ecosystems will reshape how organizations detect, analyse and model risk. However, CROs also reiterated that the value of these technologies will ultimately depend on human judgement. As machines become better at processing information, the comparative advantage of the CRO will increasingly lie in interpretation,

communication, ethical judgement and the ability to connect insights across functions, stakeholders and strategic priorities.

This evolution also changes how risk management success is measured. Historically, success was often defined by compliance, absence of loss or effectiveness of controls. Increasingly, success may be measured by how effectively the risk function enables better strategic decisions, accelerates responsible innovation and strengthens organizational resilience. In this sense, the CRO becomes not simply a guardian of the organization, but a catalyst for its long-term adaptability and competitiveness.

The future of risk management is about continuously sensing change, considering alternative futures, integrating intelligence across functions and making better decisions under uncertainty. Ultimately, the organizations that thrive in 2035 will not be those that are best at predicting the future. They will be those that are best prepared to navigate it.

Contributors

Centre for the New Economy and Society

Grace Atkinson

Insights Specialist, Global Risks Initiative

Mitali Chatterjee

Lead, Global Risks Initiative

Mark Elsner

Head, Global Risks Initiative

Saadia Zahidi

Managing Director, World Economic Forum;
Head, Centre for the New Economy and Society

Acknowledgements

The authors would like to also express their gratitude and appreciation to the members of the World Economic Forum's CRO Community who generously contributed their thought leadership and perspectives through a set of consultations. The paper does not reflect the views of these individuals and/or their organizations. The opinions are purely consultative in nature and do not imply any association with the analysis or conclusions presented within this paper.

Barbara Badoino

Head, Corporate Ethics, Risk and Compliance, Novartis

Lisa Bechtold

Chief Risk Officer, Nestlé

Christos Christou

Chief Risk Officer, LuLu Financial Holdings

Diane Doering

Global Head, Enterprise Risk Management, Takeda

Natasha Fields

Chief Risk Officer, World Trade Organization

Paul Gibson

Partner, Heidrick & Struggles

Bhaskar Mehta

Chief Risk Officer, GFH Financial Group

Qiniso Mthembu

Group Chief Risk Officer, Johannesburg Stock Exchange (JSE)

Torben Oeder

Head, Group Risk Management, Volkswagen

Monica Morata Videira

Head, Enterprise Risk Management, SAP

Damian Vogel

Chief Risk Officer, UBS

We would also like to express our gratitude to members of the CRO Community for their participation in the survey and for sharing their guidance and ideas for this paper at our workshops and events.

Production

Louis Chaplin

Designer, Studio Miko

Rose Chilvers

Designer, Studio Miko

Laurence Denmark

Creative Director, Studio Miko

Sophie Ebbage

Designer, Studio Miko

Oliver Turner

Designer, Studio Miko

World Economic Forum Public Engagement

Maxwell Hall

Creative Editorial Lead

Floris Landi

Design Lead

Sybille Penhirin

Head, Video and Design

Endnotes

1. KPMG. (2025). *Emerging Risks: Rethinking Risk Management* <https://kpmg.com/xx/en/our-insights/ecb-office/emerging-risks-rethinking-risk-management.html>.
2. World Economic Forum. (2026). *Global Risks Report 2026*. <https://www.weforum.org/publications/global-risks-report-2026/>.
3. Zhang, X., Ba, X. & Li, B. (2026). Cyberattacks in supply chains: A multi-case study. *PLOS One*, vol. 21, no. 5. <https://doi.org/10.1371/journal.pone.0350010>.
4. Łukaniszyn-Domaszewska, K., Mazur-Włodarczyk, K. & Łukaniszyn, M. (2025). Unveiling the interrelations between migration, climate change, and energy transitions in the context of socioeconomic disparities. *Energies*, vol. 18, no. 7. <https://doi.org/10.3390/en18071625>.
5. Liu, H., Renn, O. (2025). Polycrisis and Systemic Risk: Assessment, Governance, and Communication. *International Journal of Disaster Risk Science*, vol. 16, pp. 526–549. <https://link.springer.com/article/10.1007/s13753-025-00636-3#citeas>.
6. EY. (2025). *How Can Reimagining Risk Prepare You for an Unpredictable World?*. https://www.ey.com/en_gl/insights/consulting/how-can-reimagining-risk-prepare-you-for-an-unpredictable-world.
7. Accenture. (2025). *Reinventing Risk Management*. <https://www.accenture.com/ch-en/insights/consulting/reinventing-risk-management>.
8. Protecht. (2025). *Continuous Risk Monitoring: Best Practices for Complex Risk Management*. <https://www.protechtgroup.com/en-gb/blog/continuous-risk-monitoring-best-practices-for-complex-risk-management>.
9. Redis. (2025). *AI Risk Analysis and Continuous Monitoring Infrastructure*. <https://redis.io/blog/ai-risk-analysis-continuous-monitoring-infrastructure/>.
10. World Economic Forum. (2025). *AI in strategic foresight: Reshaping anticipatory governance*. <https://www.weforum.org/publications/ai-in-strategic-foresight-reshaping-anticipatory-governance/>.
11. Global Association of Risk Professionals (GARP). (2025). *Say Hello to Your Little Friend: Leveraging Digital Twins for Risk Management*. <https://www.garp.org/risk-intelligence/culture-governance/say-hello-little-friend-251212>.
12. Ghaffarian, S. (2025). Rethinking digital twin: Introducing digital risk twin for disaster risk management. *Natural Hazards*, no. 79. <https://www.nature.com/articles/s44304-025-00135-x>.
13. Logan, T. et al. (2026). Advancing Systemic Risk Assessment for Complex, Interdependent Systems: A Research Agenda. *Risk Analysis*, vol. 46, issue. 5. <https://onlinelibrary.wiley.com/doi/10.1111/risa.70243>.
14. Noona, J. (2026). AI risk analysis: *Continuous monitoring as critical infrastructure*. Redis. <https://redis.io/blog/ai-risk-analysis-continuous-monitoring-infrastructure/>.



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum is the trusted global platform for public-private cooperation, bringing together leaders from business, government, civil society, international organizations, academia and the next generation to turn foresight and dialogue into meaningful action on the world's most pressing challenges.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org