

Just in Time

Risk Management, Reimagined: Outlook to 2035

October 2026



Executive Summary

- The World Economic Forum (WEF) white paper [Risk Management, Reimagined: Outlook to 2035](#) examines how enterprise risk management (ERM) must evolve in an increasingly interconnected, fast-moving and uncertain risk environment. Based on consultations and a survey of the WEF Chief Risk Officers (CRO) Community, it argues that traditional approaches remain valuable but are no longer sufficient on their own. Risk management must therefore move from a periodic, control- and compliance-oriented discipline towards a **continuous, intelligence-driven and strategically embedded organizational capability**.
- The paper's central message is that organizations should focus less on predicting individual disruptions and more on their **capacity to operate when assumptions fail**. This requires changes to methodologies, technology, governance, scenario planning, AI adoption and the connection between risk management and business strategy.



At a Glance



01	<u>Why Risk Management Must Evolve</u>	4
02	<u>The Evolving Role of the CRO</u>	9
03	<u>Building the Risk-ready Organization</u>	14
04	<u>Conclusion & Take-aways</u>	18

Keywords: Enterprise Risk Management

01

Why Risk Management Must Evolve

Traditional Risk Frameworks Are Becoming Less Reliable

Risks Are Increasingly Interconnected

Preparedness, not Prediction, Should Become the Core
of Future Risk Management

Evolution beyond Shared Governance, Risk and
Compliance Roots



Why Risk Management Must Evolve 1/4

Traditional Risk Frameworks Are Becoming Less Reliable

Modern ERM developed in conditions broadly favourable to conventional modelling: globalization, comparatively stable geopolitical relationships and growing confidence in data-driven approaches. Traditional frameworks therefore focused on identifying threats, estimating probability and impact, and establishing controls.

The paper stresses that these techniques **remain valuable**, particularly for familiar risks for which meaningful historical information exists. The problem is therefore not that traditional risk management has become obsolete, but that its underlying assumptions are increasingly challenged by emerging risk conditions.

Many organizations continue to rely on historical data, probability assessments and periodic reviews. However, emerging technologies, geopolitical shifts and environmental developments are producing risks with limited precedent, making past relationships a less reliable guide.

This is visible in banking: observed default rates and past downturns are useful for conventional credit risk, but less informative for risks such as AI-enabled cyberattacks on real-time payment infrastructure or geoeconomic fragmentation.

Speed is another challenge. Geopolitical events, regulatory changes, cyber incidents and technological disruptions can materialize within hours, making **risk velocity** as important as risk category.

Annual or quarterly assessments may therefore become inadequate for some categories of emerging risk. Risk management must increasingly be capable of generating relevant intelligence as circumstances evolve.

The survey results demonstrate the preparedness gap. **Only 10% of CRO respondents characterize their organizations as very prepared for risks that cannot be modelled from historical information**; 47% describe themselves as moderately prepared, 37% as somewhat prepared, and 3% each as poorly prepared or not prepared at all.

Why Risk Management Must Evolve 2/4

Risks Are Increasingly Interconnected

A second structural challenge concerns the increasing interdependence of risks.



Traditional ERM commonly separates risks into categories such as financial, operational, technological, geopolitical and environmental risks. Such classifications remain useful for organizational purposes, but they can obscure the relationships between risks.



The paper argues that recent disruptions show risks can **reinforce and amplify each other**. A shock in one domain can change the probability, severity or trajectory of risks elsewhere.



For example, a cyberattack on critical infrastructure can trigger supply-chain bottlenecks, inflationary pressures and political responses. A climate disaster can simultaneously affect energy infrastructure, commodity markets and migration.



Organizations therefore confront a **dynamic system of interacting shocks** rather than simply a portfolio of independent risks.



The CRO consultations consequently emphasize the importance of understanding **risk interdependencies and propagation mechanisms**: how a vulnerability in one part of an organization or external ecosystem can affect other areas and how an external shock can cascade through interconnected systems.



The survey evidence is particularly significant. More than 70% of participating CROs place both the **inability to manage interconnected risks** and **overreliance on historical data and models** among the top three limitations of current risk-management approaches.

Why Risk Management Must Evolve 3/4

Preparedness, not Prediction, Should Become the Core of Future Risk Management

The increasing difficulty of predicting novel and interconnected disruptions leads to one of the paper's central conclusions: **preparedness should become more important than prediction.**

This does not imply abandoning quantitative models, forecasting or probability assessments. Instead, organizations should complement them with capabilities that remain effective when models fail, assumptions cease to hold or unexpected circumstances materialize.

The paper compares this concept with aviation safety. Pilots cannot anticipate every possible emergency, but they can develop procedures, governance arrangements, training and decision protocols that enable them to respond effectively to unforeseen situations.

Likewise, organizations cannot identify every future disruption in advance. They can, however, establish the organizational capabilities necessary to adapt quickly when disruption occurs.

Resilience under this model therefore becomes less dependent on the accuracy of individual forecasts and more dependent on **organizational adaptability, governance quality, decision discipline and crisis-response capacity.**

Why Risk Management Must Evolve 4/4

Evolution beyond Shared Governance, Risk and Compliance Roots

Risk management consequently needs to operate as a **strategic capability in its own right**, rather than merely as an extension of compliance.

Risk perspectives should therefore be integrated more systematically into strategic planning, capital allocation, technology investments, market-entry decisions and major business transformations.

This represents a wider conceptual change. Rather than viewing risk management primarily as a mechanism for reducing uncertainty, organizations need to recognize that uncertainty cannot always be eliminated and can itself generate strategic opportunities. The future function should therefore help organizations navigate uncertainty with greater confidence, resilience and strategic clarity.

02

The Evolving Role of the CRO



The Evolving Role of the CRO 1/4

Traditionally, the CRO has acted principally as a guardian of organizational discipline, monitoring exposures and ensuring the effectiveness of controls. The paper anticipates a considerably broader role by 2035, with CROs increasingly involved in strategy, technology, resilience and business decisions.

When asked how the CRO role is expected to change over the next five to ten years, **40% of respondents ranked playing a larger role in strategic decision-making first**, while **33% ranked becoming more technology- and data-driven first**.

Shape strategy instead of reviewing it

Instead of reviewing decisions after strategies have been formulated, CROs should participate **during strategy formation**. Their contribution should include challenging assumptions, assessing alternative pathways and identifying vulnerabilities before important decisions become final.

The survey provides strong support for this direction. **80% of respondents place embedding risk into strategic decision-making among the three most critical capabilities for the future of risk management**.

Generate risk intelligence and enable business velocity

The future CRO is also expected to move from cataloguing risks towards providing **continuous, actionable risk intelligence**.

In a rapidly changing environment, this means identifying weak signals, interpreting emerging developments and assessing how changes in the external environment could affect organizational priorities.

The Evolving Role of the CRO 2/4

Generate risk intelligence and enable business velocity

The paper draws an important link between risk management and **business velocity**. Risk functions have at times been perceived as slowing decisions through controls and review processes. Future CROs may instead be expected to help organizations make responsible decisions more rapidly.

This could ultimately affect performance measurement. In addition to traditional risk-management indicators, future CROs might be assessed according to decision turnaround time, organizational efficiency and client outcomes.

The implication is not weaker risk management, but faster incorporation of high-quality risk intelligence into business decisions.

Validate assumptions, not only risk scores

Traditional frameworks often focus on assessing the probability and impact of identified risks. The paper proposes complementing this practice by systematically examining the **assumptions underlying strategy**.

The relevant question therefore becomes not only "What risks does the organization face?" but also: **What conditions must remain true for the strategy to succeed?**

The paper cites the practice of "assumption auditing", involving systematic identification and stress testing of assumptions underpinning strategic decisions.

This approach can reveal vulnerabilities that conventional risk scoring may not capture. A strategy may appear viable under the organization's central assumptions but become significantly less robust if one or more foundational assumptions cease to hold.

The Evolving Role of the CRO 3/4

Build capabilities to adapt to, not just mitigate, disruption

Future CROs therefore need to strengthen the organization's **capacity to adapt**. This requires clear communication of uncertainty, translation of complex information into actionable insights, stronger governance and decision discipline, and more robust crisis-response and resilience capabilities.

Risk management consequently shifts from an aspiration to eliminate disruption towards ensuring that the organization can continue making effective decisions and recover when disruption occurs.

AI to complement human intelligence, not substitute it

AI is expected to transform risk management by improving pattern identification, monitoring, aggregation and predictive capabilities. Nevertheless, the CRO consultations consistently emphasize that **judgement and accountability must remain human responsibilities**.

Business leaders, not only risk specialists

This requires understanding **business models, market dynamics, commercial considerations and investment decisions** alongside conventional risk methodologies.

The paper provides a hypothetical picture of a CRO's working day in 2035: reviewing an intelligence platform that monitors geopolitical conditions, climate indicators, cyber threats, regulatory developments and operational data, and determining what those signals mean for the organization.

The Evolving Role of the CRO 4/4

Business leaders,
not only risk
specialists

Six core skill sets for the 2035 CRO:

1. **Intelligence synthesis**: combining diverse internal and external signals to identify risks and opportunities.
2. **Scenario thinking**: using simulations to test assumptions and explore alternative futures.
3. **Risk interpretation**: translating complexity and uncertainty into priorities connected with business outcomes.
4. **Stakeholder communication**: communicating risk intelligence clearly to build understanding, trust and action.
5. **Resilience leadership**: strengthening organizational adaptability, response and recovery.
6. **AI governance**: overseeing responsible AI use, including transparency, fairness, security, ethics and alignment with business objectives.

The overall profile is therefore substantially broader than that of a traditional risk-control specialist.

03

Building the Risk-ready Organization



Building the Risk-ready Organization 1/3

The paper stresses that transforming risk management requires more than strengthening the risk function. A **risk-ready organization** needs enterprise-wide capabilities for sensing change, rehearsing disruption, reflecting regional differences and combining technology with human judgement.

Continuous sensing and early warning

One of the clearest expected transformations is the transition from **periodic risk assessment towards continuous sensing**.

Traditional risk processes often depend on annual assessments, quarterly updates and retrospective reports. Such mechanisms remain useful, but they need to be complemented by tools that monitor emerging developments continuously.

AI, automation and advanced analytics enable organizations to monitor supply chains, financial markets, regulatory developments, cybersecurity, geopolitics and public sentiment in near real time.

The paper describes this as a move from **“pull-based” to “push-based” risk management**: systems continuously surface relevant developments instead of waiting for periodic assessments.

Survey evidence reinforces the importance of this capability: **70% of participating CROs rank real-time risk intelligence among the three most critical capabilities for future risk management**.

Building the Risk-ready Organization 2/3

Scenario planning and digital twins

Advances in simulation technologies and digital twins could allow organizations to test many combinations of geopolitical developments, regulatory changes, climate events, technological disruptions and market conditions.

The paper highlights the emergence of **digital risk twins**: virtual representations of an organization's risk environment combining real-time information, system dependencies, expert judgement and simulation.

The importance of digital risk twins is their ability to model **interactions between risks**. Instead of treating individual exposures separately, they can help identify hidden vulnerabilities and explore how shocks might cascade through interconnected organizational systems.

Simulation enables organizations to **experiment with uncertainty safely**, test interventions under different conditions and identify second-order effects that conventional assessments might overlook.

AI-enabled digital twins are already being applied to simulations of floods, infrastructure failures and other complex disruptions. The paper expects similar techniques increasingly to be applied to supply chains, business models and geopolitical exposures.

Recognizing and integrating regional nuances

The paper emphasizes that risk-management capabilities cannot be entirely standardized globally because regional experience influences institutional expertise and risk culture.

Different regions have historically encountered different forms of risk, shaping institutional expertise, regulatory expectations and risk culture. Climate risk provides another example: AI adoption requires data-centre capacity, electricity and cooling infrastructure, so local resource constraints should be reflected in risk assessments.

Building the Risk-ready Organization 3/3

Just in Time

Recognizing and integrating regional nuances

The paper consequently highlights the importance of **early engagement with regulators in innovation processes**, particularly where new risk-management technologies or practices need to balance innovation, market integrity and regulatory requirements.

Balancing AI and human intelligence

AI has particular advantages where organizations need to process large quantities of information continuously. Relevant applications include risk sensing, anomaly detection, cyber-threat monitoring, third-party surveillance, regulatory scanning, aggregation and pattern recognition.

AI can also help overcome fragmented risk information by integrating perspectives across cybersecurity, privacy, compliance, operational resilience, climate risk and emerging technologies, thereby identifying blind spots and interdependencies. AI cannot fully account for unique geographical circumstances, commercial realities or ethical trade-offs. Its effectiveness also depends on the quality of the processes and data to which it is applied: automating a poorly designed process does not correct its underlying weaknesses.

A further challenge concerns **preserving human expertise**. If professionals become excessively dependent on automated systems, future risk managers may struggle to develop the expertise necessary to challenge AI-generated conclusions. The strategic issue is therefore not simply **how much AI an organization deploys**, but how effectively it combines machine intelligence with human expertise.

The paper also broadens technology risk beyond software. Growing AI and quantum-computing capabilities will require greater computing capacity, data storage, electricity and cooling infrastructure. Future risk frameworks will therefore need to address the physical dependencies underpinning technological transformation, including hardware resilience, energy availability, cooling capacity and environmental sustainability.

04

Conclusion & Take-aways



Conclusion & Take-aways 1/4

The WEF concludes that ERM's traditional contribution—strengthening governance, improving transparency and reducing financial and operational losses—will remain necessary but will **not be sufficient** for the risk landscape of the next decade.

Organizations will increasingly operate under conditions in which disruption is continuous, risks interact across systems and important decisions have to be taken without complete information. Within this environment, the CRO is expected to evolve **from a risk controller towards an interpreter of uncertainty.**

AI, simulation technologies and connected data ecosystems will substantially improve the organization's ability to identify, analyse and model risks. Yet technological sophistication does not eliminate the importance of professional judgement. As machines become more effective at information processing, the distinctly human contribution becomes increasingly concentrated in interpretation, communication, ethical judgement and the ability to connect insights across functions and strategic priorities.

The paper also anticipates a corresponding evolution in the measurement of risk-management performance. Traditional measures—including compliance, control effectiveness and absence of loss—could increasingly be supplemented by measures of how effectively risk management **supports strategic decisions, enables responsible innovation and strengthens resilience.**

Conclusion & Take-aways 2/4

The resulting model of risk management is therefore continuous rather than periodic, integrated rather than siloed, and preparedness-oriented rather than dependent on accurate prediction.

ERM

Traditional ERM remains necessary but is increasingly insufficient on its own.

Historical data, probability assessments, risk registers and controls remain useful, but emerging risks increasingly lack reliable historical precedents and interact in nonlinear ways.



Structural uncertainty changes the objective of risk management.

Organizations should complement attempts to forecast specific disruptions with governance and capabilities that allow them to adapt when forecasts and assumptions fail.



Preparedness becomes more important than prediction.

The objective is not to eliminate forecasting but to ensure organizational resilience under multiple plausible futures.



Risk interdependencies require an enterprise-wide perspective.

The most material vulnerabilities may arise from interactions between cyber, geopolitical, financial, environmental, technological, supply-chain and other risks rather than from any one category in isolation.



Risk management is expected to move beyond its traditional GRC roots.

Compliance and controls remain fundamental, but risk management increasingly needs to contribute directly to strategy, capital allocation, technology investment, transformation and market decisions.

Conclusion & Take-aways 3/4

CRO

The CRO should participate in strategy formation rather than merely review completed strategies.

Risk considerations should enter decisions at inception, allowing assumptions and vulnerabilities to be challenged before commitments are made.



Assumption testing becomes a core risk discipline.

In addition to asking which risks could occur, organizations should systematically examine what needs to remain true for their strategies to succeed.



Continuous risk intelligence will increasingly complement periodic assessments.

AI-enabled monitoring can identify weak signals, anomalies and changing conditions across internal operations and the external environment in near real time.



Risk management is moving from “pull” to “push”.

Instead of relying primarily on periodic exercises to discover exposures, emerging risks can increasingly be surfaced automatically as conditions change.



Scenario planning is expected to become more dynamic.

Digital twins and simulation environments can test large numbers of interconnected scenarios and help organizations understand cascading, nonlinear and second-order effects.



Digital risk twins are principally preparedness tools, not prediction engines.

Their value lies in enabling organizations to rehearse responses and test decisions under uncertainty.

Conclusion & Take-aways 4/4

Just in Time



Regional differences remain critical.

Risk culture, regulatory requirements, historical experience, climate exposure, infrastructure constraints and geoeconomic conditions vary materially across jurisdictions and should be reflected in organizational risk capabilities.



AI will augment rather than simply replace human risk professionals.

AI is particularly suited to monitoring, aggregation, pattern recognition, anomaly detection and regulatory scanning, whereas human professionals retain responsibility for interpretation, strategic judgement, ethics, governance and accountability.



Maintaining human expertise becomes a risk-management issue itself.

Excessive dependence on automation could weaken professionals' ability to challenge machine-generated conclusions.



AI creates new physical as well as digital dependencies.

Data centers, computing hardware, energy availability, cooling infrastructure and environmental sustainability increasingly form part of the technology risk landscape.



The CRO of 2035 requires a broader skill set: intelligence synthesis, scenario thinking, risk interpretation, stakeholder communication, resilience leadership and AI governance.



Risk-management effectiveness may increasingly be judged by its contribution to organizational adaptability.

In addition to protecting against losses and maintaining compliance, the function is expected to enable better strategic decisions, responsible innovation and organizational resilience.



The paper's overarching message is that resilience does not depend on knowing precisely what will happen.

It depends on continuously sensing change, exploring alternative futures, integrating intelligence across the organization and maintaining the capacity to make effective decisions when uncertainty materializes.

ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

iason is an international consulting firm that has been supporting both financial institutions and regulators in topics related to Risk Management, Finance and ICT since 2008

Strategy

Strategic advisory on the **design** of **advanced frameworks** and **solutions** to fulfil both **business** and **regulatory needs** in Risk Management and IT departments

Methodology & Governance

Implementation of the designed **solutions** in bank departments **Methodological support** to both **systemically important financial institutions** and **supervisory entities**

Solution

Advanced **software solutions** for **modelling, forecasting, calculating** metrics and **integrating** risks, all on cloud and distributed in Software-as-a-Service (**SaaS**)

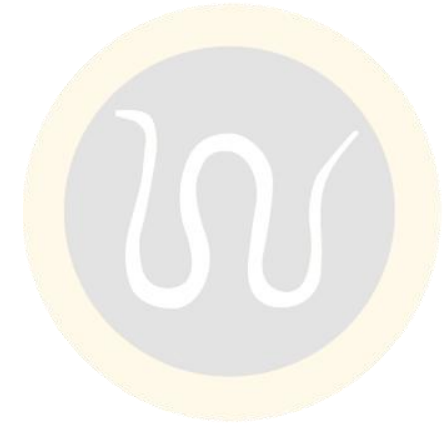
Company Profile

iason is an international firm that consults Financial Institutions on Risk Management.
iason integrates deep industry knowledge with specialised expertise in Market, Liquidity, Funding, Credit and Counterparty Risk, in Organisational Set-Up and in Strategic Planning.

Dario Esposito



Lorena Corna



This is an **iason creation**.

The ideas and the model frameworks described in this presentation are the fruit of the intellectual efforts and of the skills of the people working in iason. You may not reproduce or transmit any part of this document in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of iason.

www.iasonltd.com