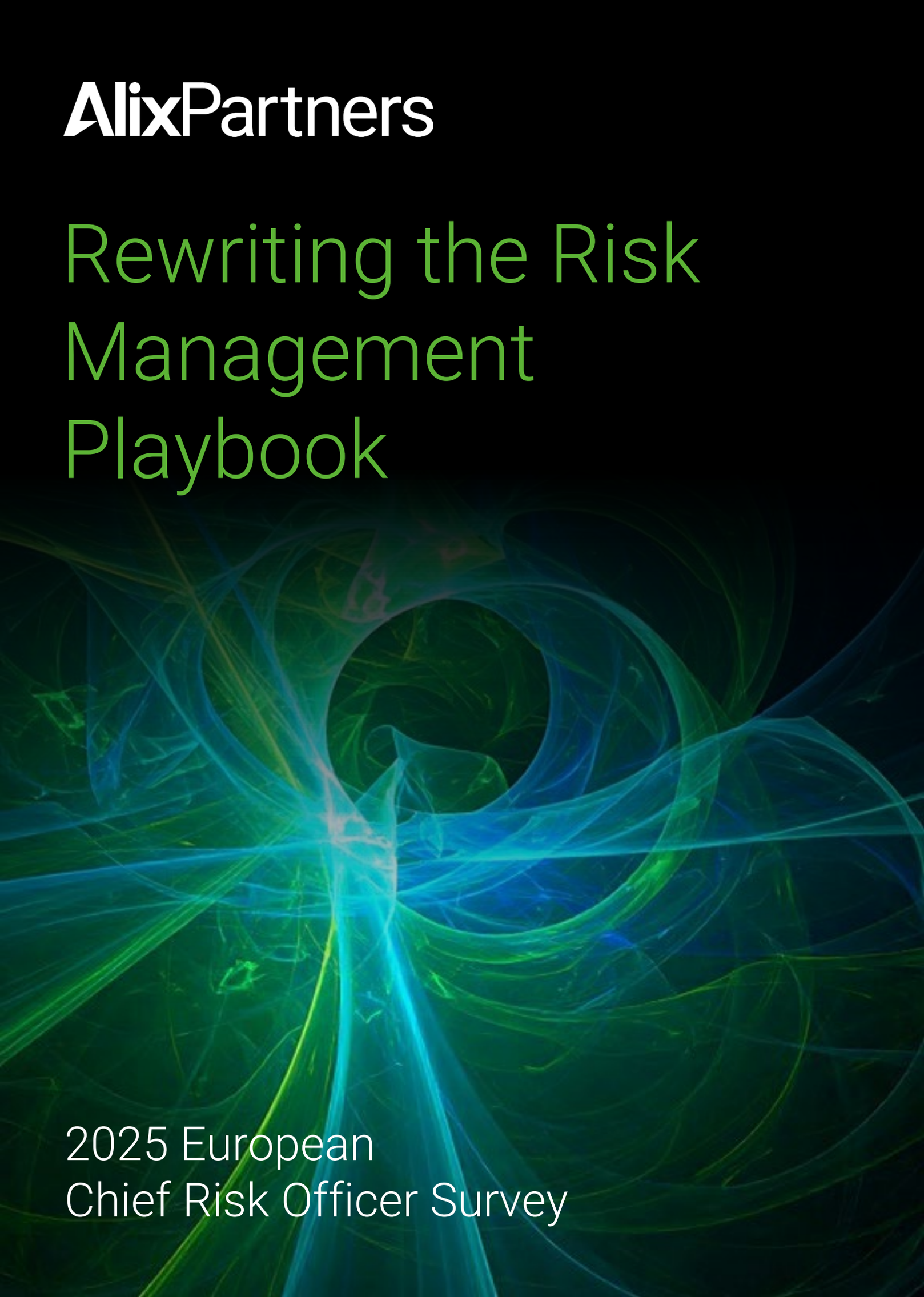
AlixPartners

Rewriting the Risk Management Playbook



2025 European Chief Risk Officer Survey

Executive Summary

This paper draws on insights from our survey and in-depth discussions in 2025 with Chief Risk Officers (CROs) at financial services institutions in Europe. These perspectives highlight the strategic priorities, challenges, and forward-looking plans that are top of mind for CROs.

Several common themes and emerging trends have surfaced, which will set the tone for 2026 and beyond. An overarching takeaway is that CROs are increasingly sounding the alarm on nth-party risks – the potential vulnerabilities and threats introduced by indirect third-party relationships, such as vendors' vendors, within a supply chain or extended ecosystem.

As financial services (FS) firms adopt more technology, automation, and cloud-based services, their supply chains are becoming longer and more complex. This means they are exposed to risks that sit several layers deep, often in places they can't easily detect or control. With regulators paying more attention to operational resilience and digital dependencies, managing nth-party risk is now a major focus area.

At the same time, FS firms are rethinking, far more regularly than was historically the case, how their Risk and Compliance teams should be organised. CROs across Europe are under increasing pressure to evolve their risk functions to respond to current and emerging risks (which are changing rapidly), accelerate digital transformation, and operate confidently in a complex regulatory environment.

Many FS firms are moving away from siloed models to build more integrated, adaptive functions, and there continues to be a shift towards far heavier focus on managing non-financial risks. They aim to integrate areas such as operational resilience, cyber, technology more broadly, and third-party oversight, enabling faster and more consistent response to new and emerging risks. CROs want Risk teams to be more data-driven, more embedded in the business, and better equipped to support business transformation and growth.

1. The shifting risk landscape

Advances in technology, growing global supply chain dependencies, and the rapid spread of risks across markets and organisations have made the risk landscape increasingly complex and interconnected. For example, as we highlight above, FS firms rely on a growing network of third- and nth-party providers, where a single point of failure can impact multiple systems and jurisdictions.

Cybersecurity and technology risk are top concerns for nearly all CROs, reflecting the growing frequency and sophistication of cyber-attacks and the sector's reliance on digital infrastructure. Credit and market risks remain significant, particularly against a backdrop of geopolitical instability, macroeconomic volatility, and diverging monetary policy paths.

A significant finding from our study was that while financial crime remains an important consideration, it no longer features among the top six priorities. In our discussions, several CROs acknowledge that it remains a high priority, though other risks have forced their way above it to the top of the agenda due to the urgent attention that they demand. These include cyber threats, climate risk, and strengthening operational resilience.

Additionally, macroeconomic volatility and regulatory divergence have further shifted focus towards credit risk, scenario testing (e.g., liquidity stress, interest-rate shocks, and sector specific downturns), and resilience planning, making these areas more immediately pressing than financial crime in today's environment, for many CROs. Firms are responding with tighter underwriting, stronger borrower-level analytics and more granular, forward-looking stress testing. This may also reflect a degree of fatigue at some organisations from the investments that have been made over the last 10 years in developing financial crime controls. That said, financial crime must remain firmly on the radar to ensure the risks arising from the evolving nature of threats are effectively managed. Regulators are sure to demand continued focus and improvements.

CROs also highlight the speed and complexity of regulatory changes, particularly in areas such as sanctions and trade risks, as an area that requires continued attention. 45% cited the operational challenge of adapting to new sanctions, and trade conflicts also are seen as a rising threat.

Top current risks

- The complex network of nth-party providers
- Cybersecurity and technology risk
- Credit and market risk (especially amid geopolitical instability)
- Reputational and conduct risk

Emerging risks for the next few years

- AI-related risks (both threat and opportunity)
- Geopolitical fragmentation and regulatory divergence
- Climate risk and sustainability
- Talent and skills shortages, especially in technology and risk analytics

2. Sanctions and regulatory divergence - a growing operational burden

Managing sanctions across multiple jurisdictions remains a significant challenge for CROs. Firms must maintain robust horizon scanning, real-time screening, and agile compliance frameworks to keep pace with evolving requirements. The operational burden of sanctions compliance is considerable, with false positives, fragmented systems, and manual interventions adding cost and complexity. These issues are compounded by the need to reconcile differing regulatory expectations across jurisdictions, which often lack harmonisation and create overlapping obligations.

Beyond sanctions, other regulatory changes continue to drive risk management activity and cost. New frameworks such as DORA, MiCA, and Basel 3.1 demand rapid adaptation, frequently with limited lead time. This places pressure on governance structures, technology platforms, and skilled resources, requiring firms to embed flexibility into compliance processes while maintaining strong oversight of ongoing compliance.

In this environment, CROs must deliver strong operational resilience while maintaining the agility to meet evolving compliance requirements. This requires scalable technology, effective cross-border coordination, and proactive horizon scanning.

3. CROs are refocusing risk functions for long-term resilience

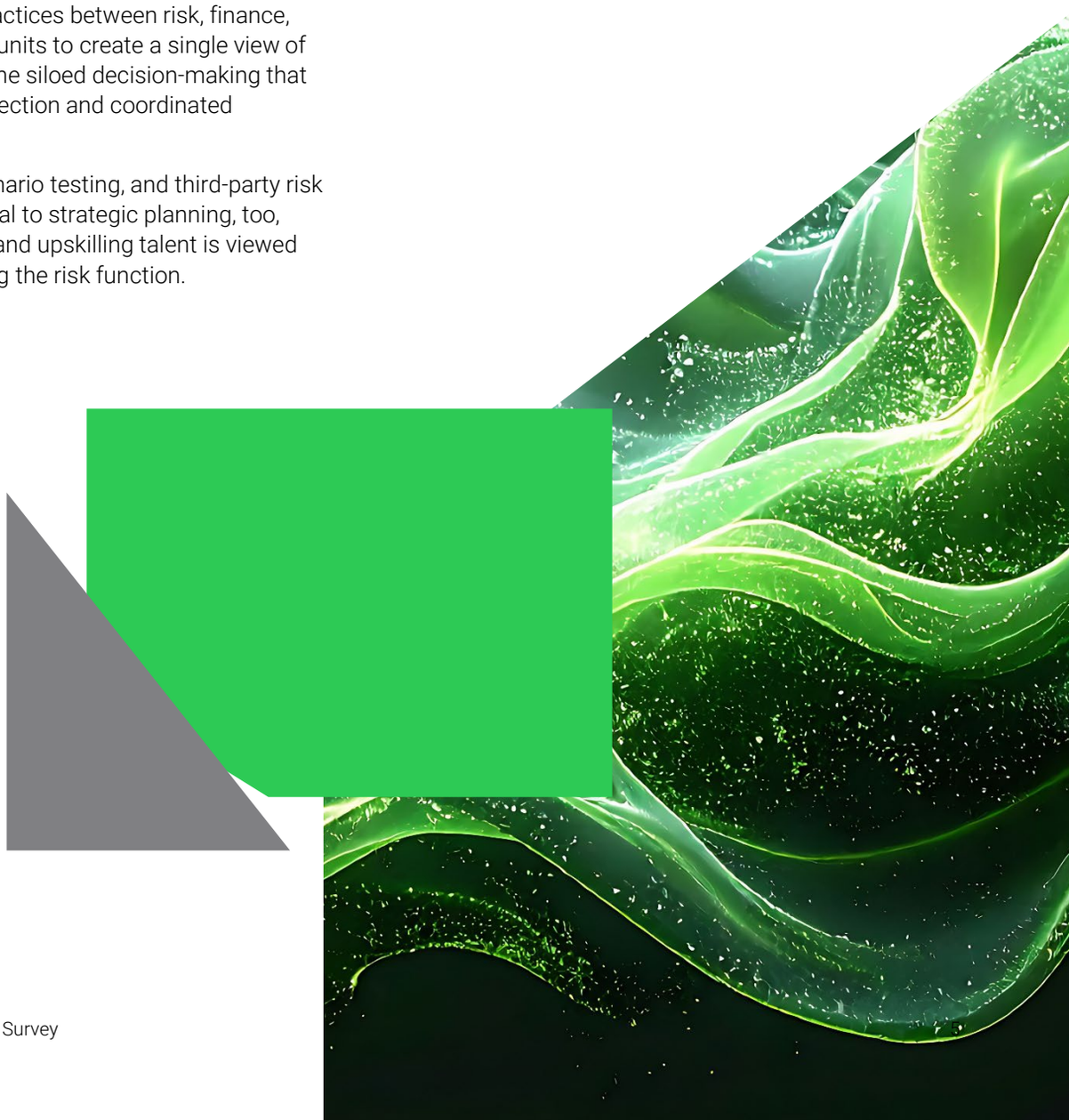
With the risk environment moving so quickly, CROs are re-examining how they manage and oversee risk. This now requires more than incremental updates triggered by crises or new regulations; it means making ongoing improvements to keep their organisations prepared.

Financial institutions are reviewing their risk management operating models regularly as the risk universe extends to include emerging threats such as climate, ESG, AI, cyber, and geopolitical risks. They are investing in bringing in new risk capabilities to cover this universe (often competing in shallow pools of talent), revising risk assessment models to incorporate dynamic stress testing and forward-looking indicators, and adopting advanced technologies to enhance predictive capabilities, such as AI-driven analytics and real-time monitoring platforms.

New ways of working are also being embedded, for example, cross-functional risk committees and more integrated data-sharing practices between risk, finance, compliance, and business units to create a single view of risk exposure and reduce the siloed decision-making that previously limited early detection and coordinated response.

Operational resilience, scenario testing, and third-party risk management remain central to strategic planning, too, while attracting, retaining, and upskilling talent is viewed as critical to future-proofing the risk function.

Although third-party risk management is relatively well established, service chain extensions have now introduced dependencies that are often opaque and dynamic. Failures at the nth-party level, such as a subcontractor of a key vendor, can cascade across critical operations, creating systemic vulnerabilities. Regulatory frameworks – such as DORA and PRA guidelines – set an expectation for firms to demonstrate resilience beyond direct vendors, necessitating continuous monitoring, contractual obligations that flow down the supply chain, and robust contingency planning. For CROs, managing nth-party risk is no longer optional; it is fundamental to maintaining disruption tolerances and safeguarding organisational resilience. There are many challenges to developing and executing risk controls in this area, and we expect more focus on this in 2026 and beyond from Boards of FS firms and regulators alike.



4. Innovation, AI and automation: early progress, significant barriers

AI adoption in risk management remains at an early stage, but is growing:

- Most firms rate current AI usage within risk functions as low (1–4/10), with a few outliers
- Common use cases include credit scoring, document review, meeting transcription, and chatbots
- Process automation is more advanced, with several firms reporting significant reductions in manual work

While AI adoption is still in its infancy, use cases are expanding and process automation is delivering tangible efficiency gains, freeing up risk professionals to focus on higher-value activities. However, significant barriers remain, particularly around data quality, integration, and regulatory clarity.

All CROs see future use cases for AI, but fewer than a third told us that they use it systematically today, mainly in pilot projects for monitoring, fraud prevention, and compliance modelling.

Integration complexity and legacy systems are key barriers:

In our view, advancing AI innovation in control functions requires a shift from isolated experiments to practical, embedded use cases that strengthen day-to-day risk management. The most effective approach is to focus on areas where AI can genuinely improve control effectiveness, such as pattern detection, anomaly identification, and faster decision support, while ensuring strong governance, transparency, and human oversight.

Progress also depends on building the right data foundations, upskilling teams to work confidently with AI tools, and creating a safe environment for testing and iterating. When implemented effectively, AI becomes less of a standalone initiative and more of a core capability that enhances resilience, efficiency, and the ability to respond to emerging risks.

UK regulatory expectations:

UK regulators have been clear that existing conduct, prudential and model-risk expectations apply to AI. CROs must ensure explainable and fair AI-driven decisions, apply consistent model governance, assess bias and unintended outcomes, and maintain operational resilience across AI systems. The direction is clear: AI requires the same discipline as any other material risk model.

5. Operating models – balancing centralisation and local adaptation

Risk operating models are evolving to balance the benefits of centralisation (efficiency, consistency, and control) with the need for local adaptation (regulatory compliance with fragmented rules and market responsiveness).

While no major shifts towards greater centralisation or decentralisation are planned, CROs emphasise the need for flexibility given factors such as geopolitical uncertainty and regulatory divergence. The most effective models are those that combine:

- Consistent enterprise-wide standards
- Clear accountability
- Local agility
- Strong data integration across functions

Conclusion

The CRO role has never been more demanding and our survey reveals a risk landscape that is increasingly complex, technology-driven, and being shaped faster than ever by external forces. While progress is being made in modernising and adapting risk management frameworks, targeted investment in AI, automation, and talent will be critical to meeting future challenges. The FS industry faces a convergence of pressures – geopolitical volatility, regulatory divergence, rapid technological change, and shifting workforce dynamics – all of which arguably need greater levels of agility and foresight from Risk leaders.

To navigate this environment effectively, CROs should prioritise the following actions:

1 **Move faster to adapt the risk operating model**

As risk drivers diversify, CROs will increasingly need adaptable frameworks that support faster, more responsive decision-making.

2 **Develop standards to manage nth-party risk**

Strengthening risk management across extended supply chains will require CROs to introduce clearer standards and monitoring approaches, supported by future regulatory developments that address deeper-tier dependencies.

3 **Adopt selected AI use cases**

Focus on efficiency and insight, ensuring strong oversight and regulatory alignment. Prioritise scalable, high-impact use cases that deliver measurable value safely.

4 **Strengthen cyber and technology risk management**

Advance monitoring, incident response, and staff capability. Invest in technology and training to stay ahead of evolving threats.

5 **Develop talent and new skills**

Prioritise upskilling, retention, and diversity in risk, technology, and analytics. Foster a culture of continuous learning and adaptability.

The pace of change demands CROs to act confidently and build capability continuously. As demonstrated by this year's shifting priorities, the challenges of tomorrow that have yet to emerge require a sustained organisational commitment to agility and adaptability across the risk ecosystem.

CROs must pair vigilance with decisive action: learning from peers across the industry, investing in the right tools, nurturing the right skills, and reshaping operating models to stay ahead.

Taking these practical steps now will build the momentum to ensure they are not only prepared for what lies ahead but are primed to shape it.

AlixPartners

Contact the authors

Munib Ali
Partner
+44 735 043 3850
syali@alixpartners.com

Tim Roberts
Partner & Managing Director
+44 776 842 4095
troberts@alixpartners.com

Gautam Sachdev
Partner
+1 212 365 8331
gsachdev@alixpartners.com

About us

For more than forty years, AlixPartners has helped businesses around the world respond quickly and decisively to their most critical challenges—circumstances as diverse as urgent performance improvement, accelerated transformation, complex restructuring and risk mitigation.

These are the moments when everything is on the line—a sudden shift in the market, an unexpected performance decline, a time-sensitive deal, a fork-in-the-road decision. But it's not what we do that makes a difference, it's how we do it.

Tackling situations when time is of the essence is part of our DNA—so we adopt an action-oriented approach at all times. We work in small, highly qualified teams with specific industry and functional expertise, and we operate at pace, moving quickly from analysis to implementation. We stand shoulder to shoulder with our clients until the job is done and only measure our success in terms of the results we deliver.

Our approach enables us to help our clients confront and overcome truly future-defining challenges. We partner with you to make the right decisions and take the right actions. And we are right by your side. When it really matters.