AlixPartners

The re-rating of Financial Services risk and the impact for CROs

2026 European Chief Risk Officer Survey

Executive Summary

The Chief Risk Officer (CRO) role has never been as visible as it is today. In a world of emerging, dynamic, and cross-cutting risks, more is expected of CROs than ever before.

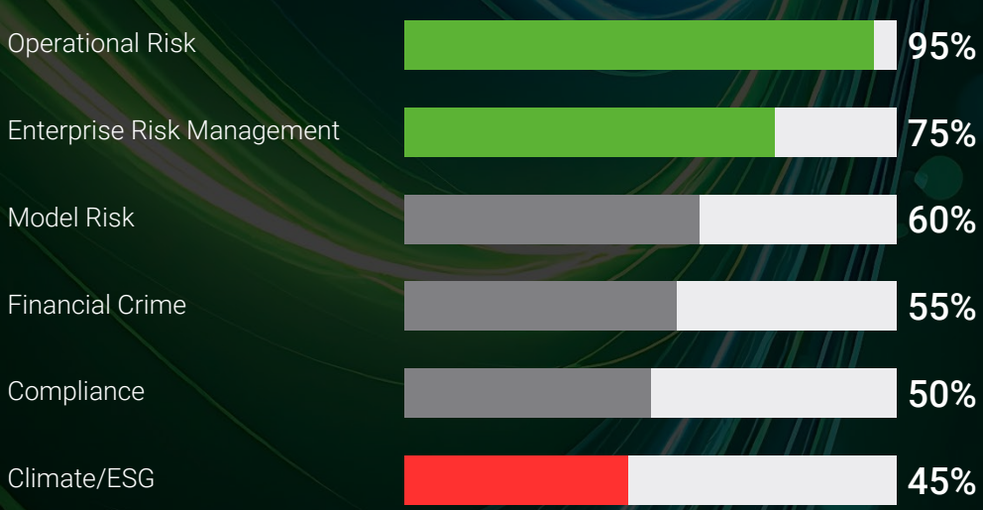
Our annual survey of European CROs shows that this widening mandate comes at a time when resources are stretched, and a disparity has emerged in how well-positioned CROs are to address the broader risks faced by Financial Services (FS) businesses.

The 2026 European CRO Survey captures views from across EMEA financial institutions, showing how risk leaders are steering organisations through new challenges in Artificial Intelligence (AI), operational resilience, third-party risk, and geopolitics.

Asked to rank their 2026 risk priorities – across financial and non-financial risk – CROs put cybersecurity, operational resilience, and model risk/AI as the top three risks, with credit and market risk now sitting outside the top five risk areas. This shift in focus has been taking place over recent years, but it's the first time that the top five has been dominated by non-financial risks. This could add to a case for consolidating the ownership of non-financial risks, rather than dividing reporting lines and potentially operating with structural gaps in which loss events could occur.

Our study shows how responsibility for non-financial risk functions currently differs across CROs. Operational risk is almost universally owned by CROs – showing the influence of operational resilience-focused regulation – while compliance, financial crime, and model risk are far less likely to report to the CRO.

Ownership of non-financial risk functions



A trend towards consolidating the ownership of non-financial risk may affect how the CRO mandate evolves. Reporting line and ownership models are, of course, very situation-specific. Outside the survey, we have recently seen instances in which non-financial risks have been consolidated outside the CRO mandate.

For some CROs, their mandate is expanding at a time when hiring intentions have halved. Just 20% of CROs plan to add headcount in 2026, down from 40% in 2025; the majority of firms anticipate seeing no change in Risk teams or a reduction in staff.

That means capacity will need to be found by leveraging technology, such as artificial intelligence (AI) and automation. But there is a gap to close regarding AI maturity, and work remains to understand where AI adds value in the CRO function.

The table below looks at where AI has been found to add value by risk area. Tasks and activities are ranked by most and least common usage, identifying where it can be used with positive results, such as speeding up the underwriting cycle or generating document packs.

Where AI adds the most value in the CRO function

AI VALUE PATHWAY	MOST COMMON →		LEAST COMMON
Operational Risk *Single-day incident triage*	**Incident triage** *Cluster & classify loss events*	**Control testing** *Sample, evidence, exception flag*	**Scenario generation** *Severe-but-plausible drafts*
Credit Risk *Faster underwriting cycle*	**Early-warning Machine Learning** *Distress signals on the book*	**Document extraction** *Covenants from filings*	**Credit memo draft** *Synthesise risk drivers*
Market Risk *Faster anomaly explain*	**Limit-breach explain** *Auto-explain PnL*	**Scenario/volatility generation** *Generate stressed market paths*	**Algorithm surveillance** *Pattern flags in trading flows*
Enterprise Risk Management *Real-time vs monthly reporting*	**Board narrative** *Risk commentary*	**KRI/KCI synthesis** *Aggregate indicators across silos*	**Regulator Q&A** *Draft responses to ad-hoc queries*
Model Risk/AI Governance *Validation pack in days*	**Validation evidence** *Auto-generate doc packs*	**Gen AI red-teaming** *Adversarial testing of LLMs*	**Challenger models** *Benchmark models to compare*
Financial Crime/AML *Lower false-positive alerts*	**Transaction monitoring** *Auto-score & dispose AML alerts*	**Name-list & sanctions** *PEP/sanctions/media*	**KYC onboarding** *ID verify, risk-rate, refresh*
Compliance *Faster horizon scanning*	**Reg horizon scan** *Map rules to obligations*	**Policy drafting** *Tailor policies to new rules*	**Conduct surveillance** *Voice/chat misconduct flags*
Climate/ESG *Build the data backbone first*	**ESG/CSRD drafting** *Pillar 3 ESG drafts*	**Transition plans** *Synthesise counterparty plans*	**Climate scenario** *Stress paths into risk taxonomy*

AI VALUE POTENTIAL:

● High ● Medium ● Low

"The rise in the priority given to non-financial risk creates new questions for CROs. The 2026 Risk Leaders Survey shows how ownership of non-financial risk varies across organisations, creating the potential for contested ground over ultimate responsibility for areas such as model risk. The key non-financial risks are interconnected, and splitting reporting lines can strain seams where loss events occur. The debate on how best to consolidate non-financial risk responsibility is likely to intensify in the coming months."

– Veit Bütterlin-Goldberg, Partner & Managing Director

"The decisions FS businesses make on AI, digital assets, and new products are some of the most consequential calls to make, yet the survey shows that not all CROs are fully embedded in these strategic decisions. Instead, some CROs are consulted on an ad hoc basis or for a narrow compliance-only view. This will need to change, given how the risk horizon is developing."

– Tim Roberts, Partner & Managing Director

Non-financial risks rise

After rising in the rankings in recent years, non-financial risks now top the risk agenda, above liquidity, credit, and market risks. This underscores the wide-ranging nature of the risk landscape and its centrality to firms' activities and decision-making.

Cyber ranks above other risks by a significant margin, jumping from 34% last year to 70% this year and represents the biggest annual change. Operational resilience and model risk/AI appear in second and third place, respectively.

Share of CROs ranking risk in top-5 for 2026

"Cyber ranks above other risks by a significant margin, jumping from 34% last year to 70% this year… the biggest annual change."

Geopolitical risk features fourth on the list, but climate and ESG has fallen from the top five, reflecting a consensus downscaling of its importance within firms, albeit not necessarily at the regulators who still expect to see climate change accounted for in credit, market, and operational risk. CROs should keep a close watch on climate and ESG, even if the spotlight has shifted for now.

In our view, this widening of the risk agenda has happened faster than many firms' operating models can adapt to, and, without specialist hiring, raises the prospect of new blind spots emerging.

Specialists in cyber, operational resilience, and AI are needed, fast. Risk functions now require security architects, model risk engineers, and third-party assurance leads, rather than relying on more traditional Risk professionals.

The top three risks must also move from narrative-only to financials. Cyber, resilience, and AI should be explicitly identified in risk appetite statements, capital planning and stress testing.

The rise in non-financial risks and changing supervisory expectations also demand developments across four areas:

- Digital and AI
- Operational Resilience
- Third-party risk and shoring
- Geopolitics

The next sections of the report explore these areas in further detail.

CROs need strategic position on AI risks

Our survey revealed that one in three CROs are being locked out of strategic decisions carrying the most material risks. When it comes to corporate decisions on AI, digital assets, and new products, 35% of CROs are only consulted on an ad hoc basis, within a limited framework, or not at all.

This percentage is particularly high, when CROs should be helping to drive the strategic agenda on such important matters.

AI and machine learning (ML) remain largely unpriced in terms of value and risk. With an average maturity score of 3.1 out of 10, the majority of CROs do not feel their organisations have sufficiently quantified the impact of AI (including generative AI)/machine learning (ML) within their organisations.

Overall maturity of technology deployment in Risk functions is low; self-rated maturity for AI and ML usage within Risk is 3.6 out of 10, on average. It is therefore no surprise that 72% of CROs say they aren't using AI broadly.

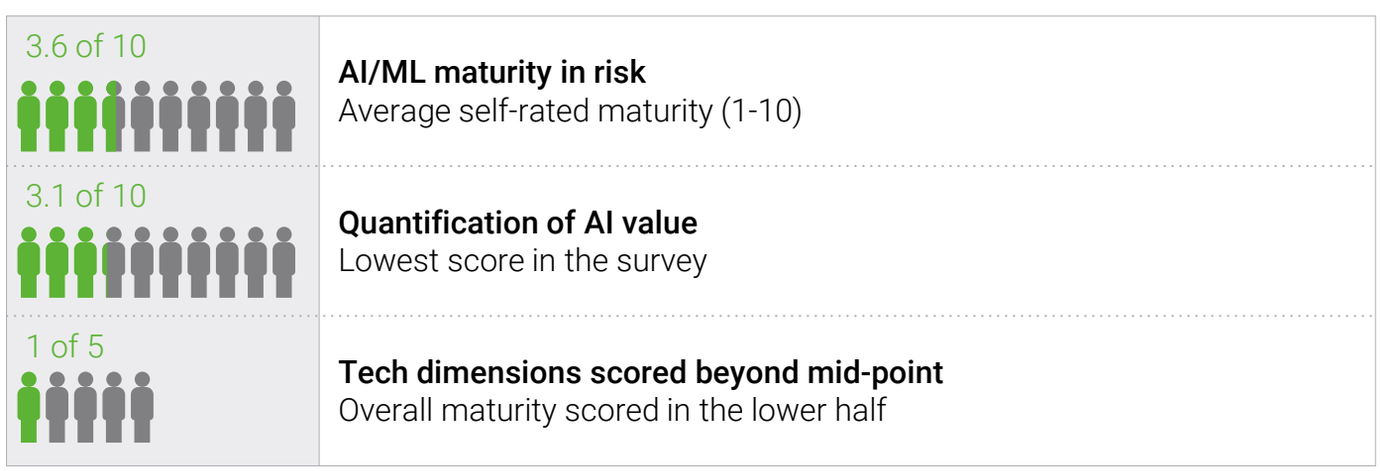
The growing risks around digital activity mean CROs should be part of strategic decision-making on AI and digital – arguably with codified veto, not just voting rights, in strategic forums.

It's now essential to integrate AI within enterprise risk and the firm-wide model risk management framework, with explicit AI-specific elements around inventory, validation, monitoring, and human-in-the-loop oversight. The absence of this will slow deployment and create ambiguity over controls application.

The gap that exists in quantifying AI value can be closed with single-name accountability and value cases, including savings, capital, productivity enhancement, and loss avoidance on all AI deployments.

Strategic involvement in AI/Digital/New products

Technology maturity



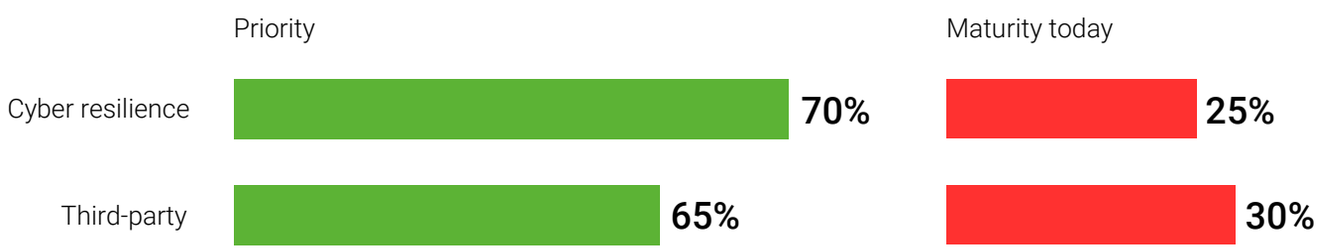
Pressure on resilience

The EU Digital Operational Resilience Act (DORA) and UK PRA/FCA regulations put heavy focus on how prepared institutions are for operational failures. While cyber risk has rapidly moved to the top of the risk ratings, the operating model hasn't kept up. Just 25% of CROs rate cyber recovery within their top three areas of operational resilience maturity.

There is also a lack of board oversight and engagement on resilience, with only 25% of boards actively steering resilience, 60% only receiving operational resilience updates, and 15% only engaging when an incident arises. Partial ownership across several stakeholders and a lack of integration within the risk framework mean resilience isn't shaping risk appetite or affecting capital decision-making.

Regulators now expect a higher standard of preparedness; they expect firms to define recovery thresholds for critical services, validated through tests. Operational resilience should be embedded in enterprise risk and have a single accountable executive, rather than shared governance.

Priority vs. Maturity — where the gap is



Vendor visibility

In last year's survey, nth party risk was identified as a resilience issue that would climb up the agenda, reflecting the different critical dependencies that exist across service chains, beyond third parties. This year, 35% assess their vendor concentration risk to be too high, and 30% said they had low or no visibility of critical vendor resilience capabilities.

Firms will need to improve vendor visibility through more frequent, risk-based monitoring of critical vendors, including control issues, incident response, financial health, and subcontractor changes, at shorter cycles than are currently in place at most firms. The market will move towards live monitoring wherever possible in the future.

As the risk framework for vendors continues to develop, risk leaders should consider setting and managing specific exposure limits by vendor, cloud provider, or country. By also using simulated exit and substitution drills, they can bring more transparency to vendor vulnerabilities, reducing the risk of high-impact incidents.

58% **Third-party framework maturity**
Self-rated, average across CROs (1-10)

45% **Will act shortly**
Plan to redraw their shoring footprint within 12 months

35% **Too many eggs in too few baskets**
Self-assess concentration risk as high

30% **Have low to no visibility**
Visibility of critical vendors' resilience capabilities – 80% low to medium

25% **Flying without an early-warning system**
Run no – or only ad-hoc/post-incident – vendor assurance

Sizing geopolitical risk

The number of CROs ranking geopolitical risk in their top five risks has climbed from 40% to 45% this year. The frequency of global conflicts and their disruption of trade and energy markets heighten these risks at an institutional level, increasing the likelihood of business interruption.

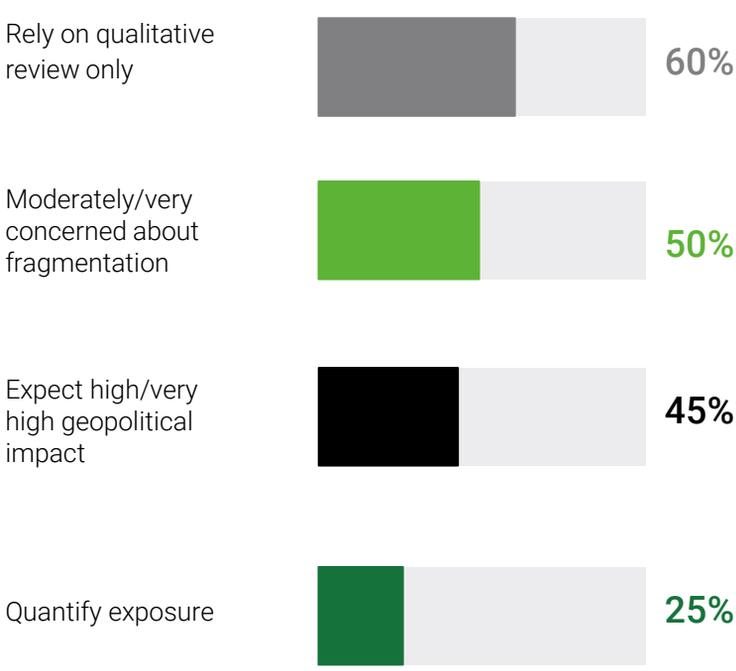
Half of CROs also anticipate continued global regulatory fragmentation linked to geopolitical risk, as some regions push ahead with deregulation while others maintain their tighter regulatory posture. Despite this growing relevance to business, 60% rely on a qualitative review of geopolitical risk, and only 25% can quantify geopolitical exposure.

So, while geopolitics has moved from a sanctions-screening task to a top-five risk priority, its impact assessment at most firms is confined to debates and discussions.

If geopolitics is made a formal part of the risk taxonomy, it can surface in limits and capital decision-making. Quantifying named scenarios, such as sanction escalation or energy shocks, enables this risk layer to be assessed, hedged, capitalised, or accepted as necessary.

That information can, in turn, inform playbooks that allocate responsibilities and actions for the critical first 72 hours of an event response.

How CROs read the geopolitical context



"Geopolitical is one of the non-financial risks ranked in CROs' top five risk priorities.

While it commonly feeds vendor and country decisions, it is rarely sized into limits, scenarios, or capital."

Archetypes for action

Four distinct styles of CRO execution emerged from the survey: differences in approach and style that define the types of CRO roles that exist and how risk is steered in different organisations.

As non-financial risks now lead the agenda and drive more and more conversations at the board level, these four archetypes have direct relevance to how CROs can respond to the changing risk landscape.

1 Architect

- Designs the Risk operating model
- Shapes all risk pillars at board level
- Runs a modern, integrated operating model
- Reacts via codified, pre-defined playbooks

2 Vanguard

- Leads on selected risk areas, typically operational resilience and third-party risk – and follows on others
- Runs cross-functional programmes
- Reacts in a structured, topic-by-topic way as priorities surface

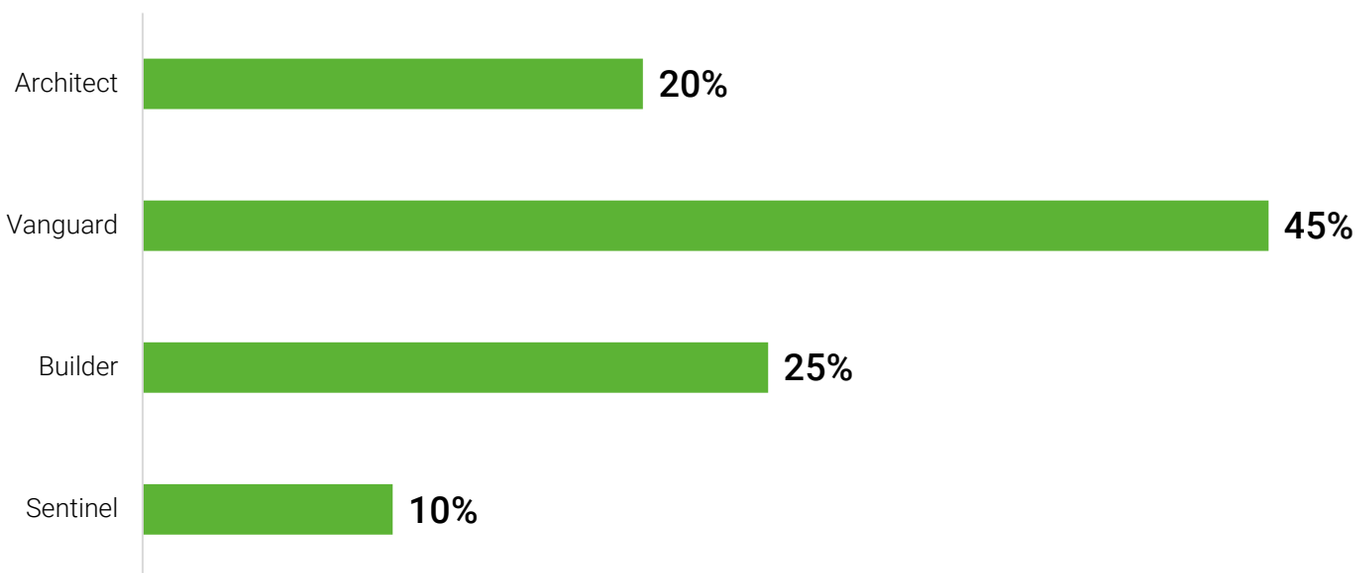
3 Builder

- Builds capability with a mandate that is expanding into nascent areas like AI and geopolitics
- Coordinates change through task forces
- Reacts tactically to audits and regulatory triggers

4 Sentinel

- Delivers compliance within a narrow, regulator-defined mandate
- Coordinates limited activities across siloed risk tools
- Reacts mainly to events and regulatory findings

Approximately 70% of firms fall within the central Vanguard and Builder CRO archetypes, characterised by selective leadership and expanding mandates, while the smallest archetype is the more narrowly-focused Sentinel at 10%. The Architect category, which plays a lead role across all risk themes, accounts for 20% of CROs.



The moves to make

As the spotlight on the CRO gets brighter, mandates continue to expand and the ability to manage increasingly complex risks struggles to keep pace. Firms should therefore be strategically considering the actions needed to position themselves most effectively for this evolving landscape. Some actions are relevant across all risk functions and CRO settings, while others should be tailored to the specific archetype represented by the CRO.

Five 'no regrets' moves all CROs can make: These are common areas where scarce capital and management attention can be spent to effectively guide risk management through the next 12-18 months.

1 **Build the economic case for AI**

Set a value target for each AI use case, route every model through a single governance lane, and bring AI under an expanded model risk management framework.

2 **Prove recovery**

Define tested recovery tolerances per important business service, name a single management-board owner, and embed resilience in enterprise risk – not next to it.

3 **Limit third-party residual risk**

Move critical vendors towards more frequent monitoring, set explicit concentration limits in the risk appetite, and demonstrate the feasibility of exiting the most critical providers through simulated drills at least once a year.

4 **Quantify geopolitical risk**

Put a number on specific geopolitical risks to move geopolitics from a narrative state into quantified risk across the full taxonomy: credit, market and operations limits, and capital. Run quantified scenarios with pre-positioned 72-hour playbooks.

5 **Reshape the CRO function**

Most CROs will see no FTE changes or will shrink teams, even as their agenda continues to expand. Institutions will find value in consolidating the ownership of non-financial risks. CROs may also need to leverage technology to boost capacity while also recruiting specialists in key cyber, AI, and resilience roles.

Actions by archetype

Our analysis of different archetypes allows CROs to self-identify which type they fall into and use this to consider more tailored, practical actions to advance risk management.

	Digital & AI	Operational resilience	Third-party & shoring	Geopolitics
Architect 20% of CROs	• Industrialise AI inside the Risk function itself • Codify methods and lead industry working groups	• Run cross-firm severe-but-plausible drills with peers • Push tested tolerances down to all subsidiaries	• Lead joint exit and substitutability tests with critical cloud providers • Share concentration data with regulators	• Translate geopolitical scenarios into capital, hedging and country limits • Brief the board with quantified loss paths, not narratives
Vanguard 45% of CROs	• Define an AI policy, owner, and approved use-case list • Run two safe pilots in a sandbox with human-in-the-loop	• Identify important business services and their dependencies • Run a first tabletop on cyber and a critical vendor outage	• Inventory critical vendors and lock exit/assurance clauses • Independently assure the top 5 vendors this year	• Map the country, counterparty, and sanctions exposure of the book • Add geopolitics to the risk register with a named owner
Builder 25% of CROs	• Productionise 2 or 3 AI use cases with measured FTE/P&L impact • Extend model-risk management to GenAI under 3LoD	• Set tested impact tolerances per important business service • Wire op-res signals into ERM dashboards and risk appetite	• Move critical vendors to continuous monitoring, not annual reviews • Run live exit drills on the top 5 vendors annually	• Build 2 or 3 named geopolitical scenarios (e.g. Taiwan, sanctions, energy) • Run them through firm-wide stress testing
Sentinel 10% of CROs	• End AI sprawl: route every use case through one governance lane • Productionise the safe ones; retire shadow models	• Replace tabletop reviews with live recovery drills • Report recovery time vs tolerance to the board, not framework status	• Set explicit vendor, cloud, and country concentration limits • Move from annual checks to risk-based continuous assurance	• Elevate geopolitics from committee debate to a named principal risk • Define transmission channels into credit, market and op-risk

Non-financial risks are no longer emerging; they are dominant. And with that dominance comes clarity: the CROs who actively shape their mandate within their organisational context, consolidate fractured ownership, and embed risk into the moments that matter most will define their institutions' resilience and performance.

Each CRO archetype, whether Architect or Sentinel, is shaped by firm strategy, board engagement, resources, and culture. The most effective CROs are those who translate emerging risks - from AI and resilience to vendor risk and geopolitics - into decisive action. The next 12 months will reveal which institutions have empowered their CROs to lead through volatility, rather than simply oversee it.

AlixPartners

Contact the authors

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

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

Dr. Veit Bütterlin-Goldberg
Partner & Managing Director
Munich
vbuetterlin@alixpartners.com

Stefan Albust
Director
Munich
salbust@alixpartners.com

Daniel Mikkelsen
Partner & Managing Director
London
Daniel.mikkelsen@alixpartners.com

James Williams
Senior Vice President
London
james.williams@alixpartners.com

Dr. Stefan Duderstadt
Partner & Managing Director
Munich
sduderstadt@alixpartners.com

Sophia Hudetz
Vice President
Zurich
shudetz@alixpartners.com

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

Leonard Funke
Consultant
Düsseldorf
lfunke@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.