RISK MANAGEMENT AND COMPLIANCE

# At Financial Institutions, Risk Should Be Everybody's Business

By Gerold Grasshoff, Rowena Fell, Anne Kleppe, Laurin Frommann, Amine Benayad, Vanessa Lyon, Kirsten Rulf, Or Klier, and Stefan Bochtler

**ARTICLE** OCTOBER 30, 2025 12 MIN READ

For decades, risk management in banking meant measuring financial exposures. Credit models, liquidity metrics, and capital buffers defined the role of the chief risk officer and formed the foundation of institutional governance. That foundation still matters. But the risks shaping financial services today are broader, faster moving, and far more interconnected than traditional tools can capture.

Five areas now dominate the risk agenda: geopolitics, regulation, digital and technology, cyber, and sustainability. These forces move across borders and functions, influencing capital, operations, and reputation all together. A regulatory change can accelerate technology adoption; a geopolitical rupture can amplify cyber threats; a climate event can test both liquidity and supply chains.

In this environment, risk and compliance can no longer operate as narrow specialties. They must function as enterprise capabilities—embedded in strategy, linked across functions, and owned by leadership as a whole. Boards, regulators, and investors are already calling for them. The financial services organizations that meet the demand will not only strengthen resilience but also gain a clearer, more immediate view of opportunities as conditions shift.

> Risk and compliance can no longer operate as narrow specialties. They must function as enterprise capabilities—embedded in strategy, linked across functions, and owned by leadership as a whole.

# Geopolitical Volatility

The global order is moving toward multipolarity, with competing systems creating instability across markets and institutions. This turbulence has direct implications for capital allocation, supply chain architecture, and corporate strategy. It also raises the stakes for risk management, compliance, and operational resilience more broadly.

Emerging pressures include:

- **Geopolitical Realignment.** Long-standing international partnerships are shifting. These changes are weakening traditional coordination channels and making global governance more difficult to predict. For financial organizations, the multipolar landscape raises the stakes on cross-border compliance, operational continuity, and risk signaling—especially in regions where institutional norms or policy frameworks are in flux.
- **Economic Policy Shifts.** Tariff oscillations and broader changes in trade and industrial policy increasingly shape global supply chains and cost structures. Sudden swings can upend market access for multinationals and reshape competitive dynamics within weeks.

- **Intersection with Technology and AI.** AI is both a competitive lever and a security risk, adding new layers of regulatory ambiguity and strategic tension across compliance, technology, and governance.
- **Flashpoints That Trigger Greater Uncertainty.** Ongoing conflicts continue to drive volatility in energy markets, capital flows, and sanctions regimes, with direct consequences for financial stability and corporate reputation.

Financial organizations can strengthen their preparedness by expanding how they model, test, and monitor risk. Reverse stress testing helps identify combinations of pressures that could threaten solvency or strategic position and turn contingency planning into a concrete exercise. Advanced modeling reveals how disruptions move through funding, supply chains, regulation, and talent, exposing weak points as well as potential openings for advantage. Integrating monitoring across risk, operations, external affairs, and regulatory teams ensures that early signals are visible and addressed through coordinated efforts.

# Regulatory Fragmentation

Regulation is evolving unevenly across geographies, with some oversight bodies loosening constraints to spur growth and others tightening oversight and standards. The pace of regulatory change has been striking. Just two years ago, systemic risks such as climate change topped many central bank agendas. Today, core mandates such as inflation control are a prime focus.

The financial sector now faces several distinct vectors of regulatory risk. They include:

- **Anti–Money Laundering and Know-Your-Customer Divergence.** In the US, enforcement has intensified, with the Financial Crimes Enforcement Network's beneficial ownership rule expanding transparency requirements. Europe has taken a structural approach, moving supervision to a new central body and harmonizing rules under the Anti–Money Laundering Authority. Global banks now face the trilemma of overlapping regimes, escalating compliance costs, and the need to preserve seamless onboarding.
- **Sanctions Volatility and Stress Testing.** In an environment of unstable global politics, sanctions are being created and updated more often, and they cover more sectors, entities, and technologies than in the past. New restrictions can appear overnight, targeting sectors, secondary actors, or emerging technologies. Traditional list-based screening systems often can't adapt fast enough, leaving gaps in coverage and increasing the risk of missteps.

- **Digital Assets Expansion.** Tokenized securities, decentralized finance protocols, and other digital instruments often fall between legal categories, creating compliance blind spots. Efforts such as Europe's Markets in Crypto-Assets framework and the GENIUS Act in the US offer direction, but global alignment remains limited.

Financial services institutions can strengthen their resilience to regulatory change by modernizing compliance and risk management. Automating core compliance is a first step: replacing static KYC files and manual onboarding with AI-enabled onboarding, perpetual due diligence, and risk-tiered surveillance. Compliance control towers can then harmonize global policies and reduce duplication across jurisdictions.

Sanctions management also needs modernization. Moving from reactive list-checking to predictive, pre-screening frameworks—supported by intelligent analytics, shared data environments, and unified case management—can help the financial sector anticipate and prevent breaches. At the same time, digital asset oversight must evolve. Rigorous classification by jurisdiction, wallet- and protocol-level monitoring, and advanced blockchain analytics, combined with active regulatory engagement, will help ensure consistency under the principle of "same risk, same rules."

Finally, institutions can converge compliance and operational risk through integrated regtech platforms, embedded controls, and adaptive architectures that strengthen defenses without adding unnecessary complexity.

# Digital and Technology Acceleration

The rapid rise of technology and AI is pushing financial services organizations into uncharted territory. Innovation is advancing faster than regulatory frameworks, leaving real-time gaps in oversight and systemic controls. The EU AI Act and similar global regulatory trends are moving toward a risk-based, horizontal model of AI governance, setting up a potential clash with existing bank risk management laws and best practices. Institutions have an opportunity—and a responsibility—to help shape a coherent AI regulatory approach for the sector. So far, their participation in the broader policy dialogue has been limited, and few formal mechanisms exist to study or address systemic AI risks specific to finance. At the same time, the risk profession itself is shifting. Talent once focused on credit and market exposures is being redeployed into technology and AI, bringing analytical discipline to domains that now sit at the center of institutional stability.

> The risk profession is shifting. Talent once focused on credit and market exposures is being redeployed into technology and AI, bringing analytical discipline to domains at the center of institutional stability.

There are three areas of particular concern:

- **GenAI and Agentic AI.** The acceleration of generative and agentic AI—where autonomous agents act with minimal human oversight—creates risks across the full range of financial activities, particularly non-financial categories. Oversight must extend across the AI life cycle, with governance, testing, and controls adapted as capabilities advance.
- **Third-Party Concentration.** Reliance on a small set of external providers for computation and AI capabilities raises questions about concentration risk, resilience, and control. Financial services organizations must plan for service interruption, set clear boundaries on what can be outsourced, and install effective compliance mechanisms to meet supervisory expectations.
- **Hyperscaler Dominance.** A small number of cloud providers now underpin critical banking operations, turning a once-niche outsourcing choice into a structural dependency. This creates operational and geopolitical risks. Risk, compliance, and tech leaders as well as boards need to define mission-critical zones where sovereignty must be preserved and ensure that governance forums weigh trade-offs between resilience, cost, and innovation.

Banks will need greater discipline and control in how they deploy and oversee technology. A strong AI governance and control framework is central to that goal. Each deployment should be clearly mapped—what software is running, where data resides, and which guardrails are in place—and tied directly to the institution's data strategy. Oversight should extend across the lifecycle, from design and testing to deployment and monitoring.

Third-party resilience requires the same level of attention. Organizations can plan for service interruptions, define clear outsourcing boundaries, and give compliance teams full visibility across the supplier landscape. Governance models need to support continuous oversight rather than periodic reviews. Sovereignty in mission-critical functions also matters. Areas such as liquidity management and risk engines cannot depend entirely on external hyperscalers. Institutions should identify where those dependencies exist and build internal capabilities that can operate independently when needed.

# Cyber Exposure

Cyber attacks are becoming more sophisticated, hitting both operations and reputation. These breaches range from ransomware that paralyzes services to AI-generated fraud and disinformation that spread faster than defenses can be adapted to stop them. Yet accountability for cybersecurity standards is still fragmented, with regulators, industry bodies, and institutions debating who should lead. Many stakeholders are calling for an industry-agnostic approach where state institutions, and not just financial regulators, set and enforce cybersecurity frameworks. Until clearer alignment emerges, financial services organizations will need to lead their own resilience initiatives.

> “Accountability for cybersecurity standards is still fragmented, with regulators, industry bodies, and institutions debating who should lead. Until clearer alignment emerges, institutions will need to lead their own resilience initiatives.

That means reckoning with pressing exposures on a number of fronts:

- **AI-Driven Threats.** GenAI is being weaponized to automate phishing, create adaptive malware, and evade detection, while deployments within firms often expand the attack surface without embedded safeguards.
- **Third- and Fourth-Party Risk.** As digital ecosystems expand, transactions with vendors and partners increase exposure to risk. Outages or disruptions far down the supply chain can have an enterprise-wide impact on banks. Static vendor assessments often fail to detail network dependencies and vulnerabilities.
- **Cyber Crisis Management and Readiness.** New regulations such as the EU’s Digital Operational Resilience Act and Network and Information Security Directive 2, and the US Securities and Exchange Commission’s cybersecurity rules, raise expectations. But many firms still lack enterprise-wide playbooks.

Building cyber resilience demands a coordinated approach. Security needs to be built into AI and digital systems from the start, with governance, data safeguards, and risk checks treated as design requirements rather than afterthoughts. Institutions also need a clearer view across the risk landscape. Integrating oversight, analytics, and governance for cyber, fraud, and financial crime

creates a unified model that sharpens detection, reduces redundancy, and allocates scarce talent where it has the greatest impact.

Third-party oversight also needs to evolve. Instead of static vendor assessments, financial services organizations need to continuously monitor their digital supply chain, treating ecosystem resilience as a core capability rather than a compliance exercise.

Finally, crisis readiness must move beyond the technology function and become a board-level discipline. Enterprise-wide playbooks should outline critical processes, test breach scenarios, and coordinate actions across business, legal, and communications teams. Institutions that practice these responses under stress build the organizational muscle to act decisively when disruption occurs.

# Sustainability Regulation

Sustainability has become a core regulatory and strategic issue, and the focus is shifting from voluntary commitments to measurable disclosure and shareholder value. In Europe, many banks remain committed to carbon dioxide reduction, but the context is changing. New taxonomies now classify defense and nuclear power as sustainable. Meanwhile, US regulators have eased enforcement of some environmental, social, and governance (ESG) standards. These differing approaches add complexity to the risk and compliance landscape.

The European Banking Authority's (EBA) 2025 guidelines raise the bar further. Regulators across Europe are maintaining strong pressure on banks—reinforced through warning letters and the threat of fines—to accelerate progress. The guidelines embed ESG risks directly into capital and liquidity planning, impose time-bound transition plans, expand the scope to include social and governance factors, and assign explicit board-level accountability. The result is a demanding, data-driven framework that will test systems, governance, and strategy.

The evolving agenda presents new challenges for institutions:

- **Shifting Definitions and Political Divergence.** Geopolitical forces are redrawing what counts as sustainable. In Europe, defense and nuclear power are now green-listed—while other regions adopt different taxonomies. Banks must navigate this divergence without compromising their own strategic positioning.
- **Elevated Regulatory Demands in Europe.** The EBA's 2025 guidelines introduce more prescriptive requirements, embedding ESG into capital and liquidity planning and requiring time-bound transition plans and sector-specific risk assessments.

- **ESG Beyond the "E."** Supervisors now expect institutions to treat social and governance risks with equal rigor. That means enterprise-wide reporting, board accountability, and better data infrastructure.

The financial sector needs integrated approaches to manage sustainability risk with consistency across the enterprise. Building auditable data foundations can replace fragmented reports and provide a clear, verifiable view of environmental, social, and governance exposures. They also need to incorporate ESG into capital and credit decision making. This includes aligning the Internal Capital Adequacy Assessment Process, Internal Liquidity Adequacy Assessment Process, and risk models with transition plans and board oversight. Clear decision frameworks can help balance resources across jurisdictions as regulations diverge, ensuring compliance and investment remain aligned with strategic priorities.

---

Risk has always been a central concern in banking. What has changed is its shape and speed. Geopolitics, regulation, technology, cyber, and sustainability now move together, creating pressures that extend far beyond the balance sheet. Traditional models and buffers remain important, but resilience today depends on how well institutions can connect signals across domains and respond as one.

That responsibility no longer sits with risk and compliance alone. Every function—from finance and operations to technology and strategy—has a role in anticipating shocks and managing trade-offs. The CRO and CCO remain at the center, but they are now part of a wider enterprise discipline that helps boards and executives make coherent, risk-informed decisions under pressure. Institutions that build this shared capability will not avoid disruption, but they will face it with clarity, speed, and control, earning the confidence of regulators, investors, and clients alike.

# Authors

## Gerold Grasshoff

Managing Director & Senior Partner
Frankfurt

## Rowena Fell

Senior Director - Risk & Compliance, BCG Vantage
London Canary Wharf

## Anne Kleppe

Managing Director & Partner
Berlin

## Laurin Frommann

Managing Director & Partner
Zurich

## Amine Benayad

Managing Director & Partner
Paris

## Vanessa Lyon

Managing Director & Senior Partner
New York

## Kirsten Rulf

Partner & Associate Director
Berlin

## Or Klier

Managing Director & Partner
Tel Aviv

## Stefan Bochtler

Managing Director & Partner
Munich

## ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.