CeFPro®

Connect MAGAZINE

JULY 2026

TPRM

Geopolitics

Governance

Treasury

Risk Culture

Kill or Be Killed

– Slaying the Multi-Headed Hydra of Risk

Governance Without Velocity:
Are banking risks now moving faster than decisions?

Visibility Without Context:
What are the hidden threats beyond our four walls?

Innovation Without Reliability:
Does AI confidence spell operational fragility?

Resilience Without Ownership:
Could outsourced services still be your in-house risk?

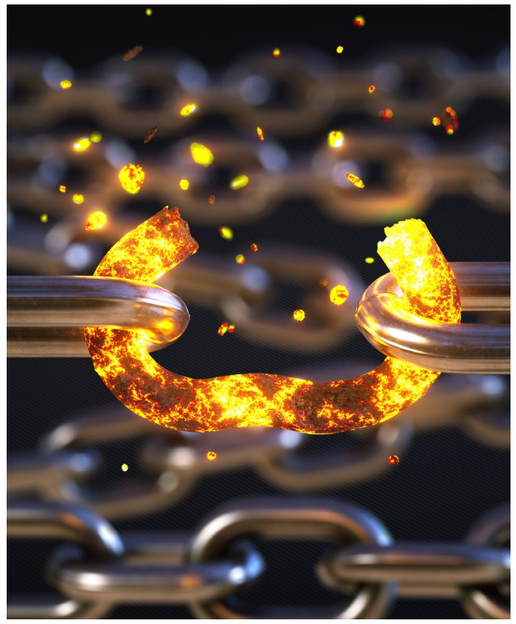
Culture Without Consequence:
What happens when incentives overpower risk appetite?

connect.cefpro.com/magazine

CONTENTS

This month's regular features in Connect Magazine

The views and opinions expressed in this publication are those of the thought leader as an individual, and are not attributed to CeFPro or any particular organization.



Magazine team —

Publisher
Andreas Simou
Managing Director
CeFPro
andreas.simou@cefpro.com

Editor
Mark Norman
Head of Content
CeFPro
mark.norman@cefpro.com

Sales & Advertising
Chris Simou
Head of Sales
CeFPro
chris.simou@cefpro.com

Marketing
Alana Cannatella
Media Marketing Manager
CeFPro
alana.cannatella@cefpro.com

Design
Natasha Marino
Head of Design
CeFPro
natasha@cefpro.com

The Dawning New Reality of Banking Risk

Andreas Simou, *CEO,* **CeFPro**

Welcome to this month's edition of Connect Magazine.

If there is a single theme running through the banking industry today, it is speed. Risks are emerging, converging, and evolving faster than many institutions can comfortably govern.

Across both financial and non-financial risk disciplines, the challenge is no longer simply identifying threats, but recognizing them early enough to act decisively.

Several articles in this issue explore that reality from different perspectives. We examine how the combination of artificial intelligence and geopolitical fragmentation is creating a new generation of interconnected risks that challenge traditional governance models.

We also look at why many institutions are struggling to separate meaningful signals from overwhelming volumes of data, and why faster, more effective risk decisioning is becoming a competitive advantage.

Elsewhere, contributors explore the growing importance of third-party risk management, the hidden operational risks that may accompany rapid AI adoption, and the danger of treating risk culture as a reporting exercise rather than a behavioral discipline.

Treasury leaders, meanwhile, argue that balance sheet resilience increasingly depends on understanding institution-specific risks rather than simply satisfying regulatory expectations.

Taken together, these articles point toward a common conclusion: resilience, adaptability, and informed decision-making have become as important as measurement, compliance, and control.

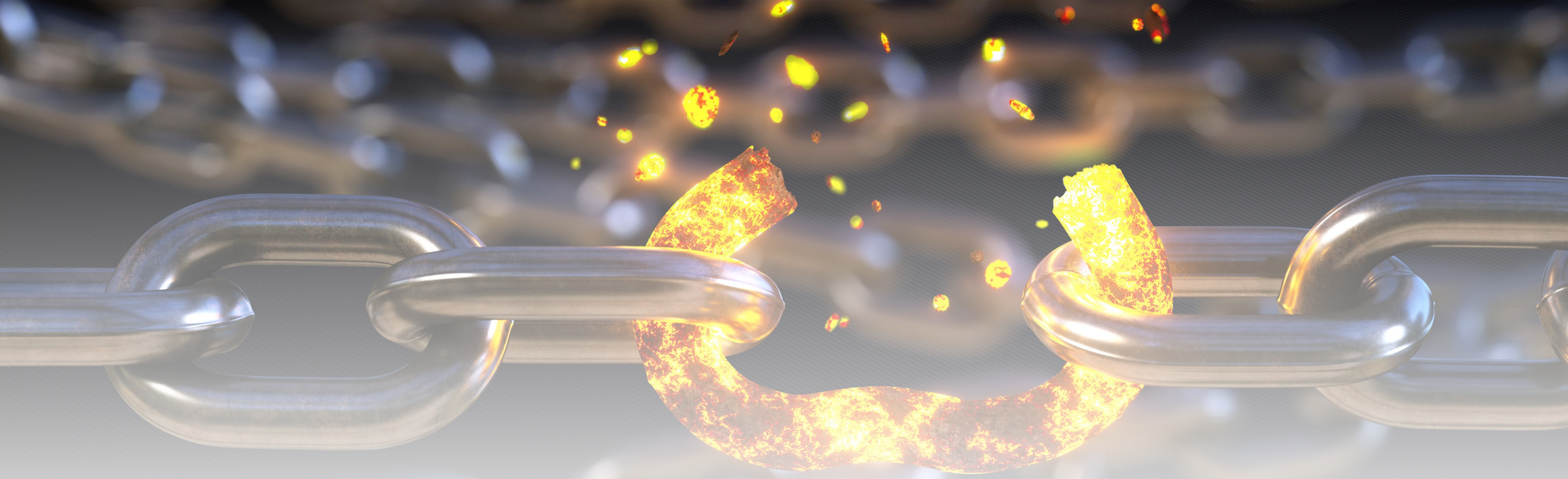
As the industry continues to navigate this environment, we look forward to welcoming many of you to CeFPro's upcoming events, including Balance Sheet Management in September and Next Gen OpRisk in November.

Early bird registrations are currently available, and I encourage you to secure your place while those offers remain open.

We are also always keen to hear from organizations interested in advertising within Connect, becoming a guest editor for a future edition, or discussing sponsorship and advertorial opportunities with our team. Our contact details can be found on page 4.

I hope you enjoy this month's articles and insights. The next edition of Connect will be published on July 25, 2026.

Andreas



BANKS MUST NOT **OUTSOURCE** THEIR MOST **DANGEROUS RISKS** – HERE'S WHY

Jenna Wells is the CEO at Supply Wisdom, a leading provider of third party risk solutions and intelligence. She has previously held senior risk management roles at Iron Mountain and Wellington Management.

Third party risk management is no longer about annual questionnaires, isolated compliance checks or static assessments sitting forgotten in spreadsheets.

According to Jenna Wells, CEO at leading risk intelligence consultancy Supply Wisdom, the speed and complexity of global disruption now means banks must rethink how they identify, monitor and respond to operational threats across sprawling supplier ecosystems.

Wells argues that the traditional model of periodic vendor assessment has effectively collapsed under the weight of geopolitical instability, cyber threats, sanctions risk and rapidly evolving artificial intelligence exposure.

"The second it's sent, it's stale," Wells says, referring to static supplier assessments. "You get that baseline as of the day it was filled out, and then you are absolutely blind."

Drawing on her experience both as a practitioner and now as a solutions provider, Wells lays out a global risk landscape that has transformed dramatically over the past decade.

Disruption is disparate, its causes manifold. Most obviously in recent years, perhaps, are the conflicts in Russia, Ukraine, and the Middle East, tensions in China and Taiwan, the global pandemic of 2020 and 2021,

But front of mind though they undoubtedly are, they are far from the only factors in an increasingly vulnerable global third party ecosystem.

Outsourcing has also accelerated aggressively across financial services. Banks now depend on vast networks of suppliers, subcontractors and technology providers spread across multiple jurisdictions and geopolitical environments.

Wells believes many institutions still underestimate how little visibility they truly possess over their global networks.

“One of the first areas where companies are fooling themselves is they don’t know the full scope of their outsourced vendor population,” she says.

According to Wells, the problem extends beyond direct suppliers. The real challenge increasingly lies within secondary, tertiary and even deeper supplier relationships that support critical operations behind the scenes.

“You can outsource the function, you can never outsource the risk,” she says.

That distinction has become increasingly important as regulators tighten expectations around operational resilience and third party oversight.

Wells points specifically to the EU’s Digital Operational Resilience Act as evidence that continuous monitoring is no longer optional for financial institutions, saying, “It’s actually now a regulatory requirement.”

She warns that many organizations continue to manage risks in fragmented silos, with separate teams overseeing cyber, compliance, ESG, operational and financial risk using disconnected tools and inconsistent methodologies.

This fragmentation, she argues, prevents institutions from identifying broader patterns and emerging vulnerabilities across their supplier ecosystems.

“When you see data across a 12 month period, across multi domains, you start to identify trends between teams,” she says.

She describes how deteriorating financial conditions at a supplier may initially appear as isolated operational issues before eventually triggering broader service disruptions, staffing reductions or security concerns.

Continuous monitoring, she argues, allows firms to detect those warning signals earlier and respond proactively.

Artificial intelligence is simultaneously creating both opportunity and risk. Wells acknowledges AI’s transformative potential but cautions that banks may be embracing the technology faster than they can properly govern it.

“AI is becoming the newest silo in risk management,” she said.

One of her biggest concerns is the widespread unofficial use of generative AI tools by employees across financial institutions.

Wells believes many organizations are already exposed to data leakage and governance risks because employees have integrated AI platforms into daily workflows long before formal oversight frameworks were established.

“That risk is already out there,” she says. “And that means you’re now in mitigation mode.”

Despite the growing focus on AI, Wells repeatedly returns to what she describes as foundational risk management disciplines, in which people are increasingly focused on AI even though they don’t fully understand their risk exposure.

> ***You can outsource the function, you can never outsource the risk.***

Or put another way, many organizations set out on finding solutions to problems that may not actually be a problem at all – or, at least, not the problem they think it is.

In this way, understanding supplier populations, maintaining accurate vendor data and identifying service delivery locations remain critical weaknesses for many firms.

“If you don’t have a true view of your outsourced population, how can you even start to determine the risk?” she asks.

For Wells, the solution ultimately depends on breaking down internal silos and embedding risk accountability across the entire organization.

She believes meaningful resilience only emerges when boards, CEOs, risk leaders and business functions operate from a unified and continuously updated view of enterprise risk exposure.

“It must start at the very, very top,” she insists.

TREASURY MUST STOP HIDING BEHIND REGULATORS

Christina Victor is Executive Director in the Capital and Balance Sheet Management team for the Americas Division of SMBC. She has previously held executive analyst and treasury roles within First Citizens Bank and EY. She holds a Finance MBA from Baruch College.

Treasury professionals have spent years concentrating on regulatory expectations, but the future of the discipline may depend on a far more fundamental question: what risks actually matter to their own institutions?

According to Christina Victor, Executive Director, SMBC Americas Division, treasury teams are entering a period where managing risk based solely on regulatory requirements is no longer enough.

Instead, institutions must increasingly focus on understanding their own unique exposures and building the flexibility needed to respond to a rapidly changing environment. Speaking at CeFPro's 2026 Risk Americas conference earlier this year, Victor said: "For a long time, we've been focused on what does the regulator need.

"We've been focused on reading the fine print in regulations, focused on things like enhancing your documentation and peer reviews to see what are others doing so we can do something comparable."

But that approach, she believes, is beginning to change.

"Now, gradually, we'll see a shift towards the question of what is our risk," Victor said. "Every bank is unique, our products are unique, our risks are unique, and we probably understand our risks better than the regulators do."

> ***Every bank is unique, our products are unique, our risks are unique.***

Drawing on more than two decades of treasury experience, including living through both the Lehman Brothers collapse and the failure of Silicon Valley Bank, Victor argues that institutions now have enough experience to move beyond simply implementing regulatory prescriptions and instead focus on managing risks that are specific to their balance sheets and business models.

"At the end of the day, we are risk managers," she said. "In this expansionary environment, we allow and help our businesses to grow by managing risks."

That shift comes at a time when treasury teams face unprecedented uncertainty. Geopolitical conflict, economic volatility, pandemics, technological disruption, and changing customer behavior have made forecasting increasingly difficult.

"Flexibility is essential with the very rapidly changing macroeconomic environment," Victor said.

But rather than attempting to predict every possible shock, she believes treasury functions must build capabilities that instead allow them to react quickly as events develop without ignoring the importance of horizon scanning to pre-empt challenges.

"We need to be able to run these ad hoc scenarios, which sometimes we don't expect," she explained. "Who expected the war? Or who expected COVID, for that matter?"

For Victor, the key question is not whether institutions can predict every crisis, but whether they can adapt when conditions change.

"We are always stress-testing," she said. "But the exact scenarios will likely be different. So are we able to pivot?"

One area where treasury assumptions are already being challenged is deposit behavior. The collapse of Silicon Valley Bank exposed how quickly customers can move funds in a digital world, creating what Victor described as nonlinear outcomes that traditional models may fail to capture.

"Some of our assumptions in terms of deposit runoff specifically were not as linear as we expected," she said, acknowledging that technology has fundamentally changed how customers react during periods of stress.

"Now I'm able to withdraw my deposit through my phone, and real-time payment systems have evolved to support that," Victor noted. "Social media spreads news so fast."

The result is what she describes as a new form of convexity in treasury risk management, where market reactions can accelerate suddenly and unexpectedly.

"In a time of stress, the reaction is nonlinear," she said. "There's a sudden, abrupt change. There's a second-order effect in it."

That requires treasury teams to rethink stress testing assumptions, liquidity buffers, recovery planning, and scenario analysis. It also means preparing for emerging risks linked to technologies such as artificial intelligence.

"There's this whole world of unknown that we need to be prepared for, and things happen pretty quickly," Victor warned.

At the same time, she believes treasury's role is expanding beyond traditional risk management. Balance sheet optimization, funding efficiency, hedge effectiveness, and risk-weighted asset management are increasingly creating tangible value for institutions.

"Treasury never thought of ourselves as a P&L center," Victor said. "But we are saving money in terms of how we optimize our funding costs, how we optimize our hedges, how we do the RWA optimizations."

As regulatory remediation efforts gradually consume less time and fewer resources, she expects treasury teams to become even more strategically important.

"Treasury will be doing more and more of it," she said.

For Victor, that future depends on remaining curious, collaborative, and open to learning from peers facing similar challenges.

"These conversations help us," she said of the Risk Americas conference. "We learn from one another, and it just helps get that industry perspective."

COMING SOON...

The Cross Industry TPRM Series

In partnership with TPRA

Join the senior **third-party risk leaders** from across **financial services, healthcare, energy, technology, telecoms** and more at the Vendor & Third-Party Risk Cross-Industry Conference Series, **in partnership with TPRA.**

Focused on **operational resilience, AI, cyber risk, regulation,** and **systemic third-party exposure,** the event is built on one core idea: the best risk strategies are often learned from industries ahead of the curve.




The Cross-Industry Series Combined in Numbers:

300+
Senior attendees

60+
Expert speakers

3
Focused content streams

20+
Presentations, panels and interactive discussions

5+
Roundtables and scenario-based sessions

Be part of the **conversation shaping** the **future of third-party risk.**

Register your interest today!

London › **Fort Worth ›**

Vendor & Third Party Risk USA

The Cross-Industry Conference

October
14-15
Fort Worth

Find out more ›

Vendor & Third Party Risk Europe

The Cross-Industry Conference

November
10-11
London

Find out more ›

How Banking Risks are Outpacing the Industry's Response Ability

Artificial intelligence, cyber threats, geopolitical instability and private credit exposures are converging to create a new generation of interconnected risks for global banks.

Recent surveys and regulatory warnings reveal growing concern among senior risk leaders that traditional controls and legacy systems may no longer be capable of responding quickly enough to rapidly evolving threats.

From AI-driven cyber attacks to hidden vulnerabilities in private markets, financial institutions are increasingly confronting a world where operational resilience, technological adaptation and risk visibility have become critical determinants of stability and survival.

74% of bank CROs rank technology and cyber risk among their top concerns

The 2026 CRO Outlook Survey by Oliver Wyman and ProSight found that nearly three-quarters of banking chief risk officers now view technology and cyber risk as a top-five threat category. Risk leaders cited AI-enabled cyberattacks, expanding digital ecosystems, legacy technology vulnerabilities and growing third-party dependencies as key drivers. The findings reflect how cyber risk has evolved from an IT concern into a core financial stability and operational resilience issue for banks globally. *Source*

95% of financial system participants cite geopolitical risk as a major threat

The Bank of England's 2026 Systemic Risk Survey found that 95% of respondents identified geopolitical risk as a significant threat to financial stability, making it the most frequently cited systemic risk. Cyberattack ranked second at 82%. The survey highlighted growing fears that geopolitical fragmentation, trade conflict and state-sponsored cyber activity could rapidly spill into banking markets, operational resilience and liquidity conditions. *Source*

31% of global data breaches now begin with vulnerability exploitation

Verizon's 2026 annual breach report found that software vulnerability exploitation overtook stolen credentials as the leading cause of cyber breaches for the first time. The report reviewed more than 31,000 incidents and concluded that AI is accelerating the speed of attacks, reducing response windows from months to hours. For banks, the findings reinforce fears that AI-enhanced cyber threats could overwhelm legacy systems and traditional security controls. *Source*

Banks globally hold hundreds of billions in exposure to private credit markets

Growing concern over opaque private credit exposures is becoming a major issue for bank risk managers. Reuters reported that regulators are increasingly worried banks may not fully understand indirect risks tied to private credit funds and non-bank financial institutions. Rising defaults and weakening loan quality in private markets are intensifying fears that hidden leverage and illiquidity could amplify future financial stress. *Source*

54% of banks already have AI operating in production environments

According to the 2026 CRO Outlook Survey, more than half of banks have now moved AI beyond pilot stages into live production environments. Meanwhile, 48% expect AI deployment within risk functions over the next two years. The rapid expansion of AI is increasing concerns around governance, model risk, explainability and operational resilience as banks attempt to balance innovation with regulatory expectations. *Source*

> ***AI is fundamentally reshaping the cybersecurity industry.***

52% of risk professionals rank AI and emerging technology as biggest threat in 2026

CeFPro's 2026 Global Risk Outlook Survey 2026 found that AI and emerging technology risk continues to be the single biggest risk facing financial institutions. Evidencing the evolving nature of that threat, respondents cited concerns around model explainability, governance, ethical use, and the malicious misuse of AI to create uncertainty in balancing innovation, resilience, and effective oversight. *Source*

72% of bank CROs say AI adoption in risk functions remains limited

The EY and Institute of International Finance Global Bank Risk Management Survey found that 72% of chief risk officers still describe AI adoption within risk functions as limited or early-stage, despite mounting pressure to modernize. At the same time, 55% said advanced technology implementation is now one of their top three priorities. The findings highlight a growing tension between accelerating AI-driven threats and banks' ability to operationalize AI safely within risk management, fraud detection, cyber resilience and real-time monitoring frameworks. *Source*

CONNECT LEADER:

HOW AI AND GEOPOLITICS ARE DISRUPTING TRADITIONAL RISK MANAGEMENT THINKING

Mark Norman is Head of Content at CeFPro. He is a journalist with more than 40 years' experience in local, regional and national newspapers across the UK, and has held various senior editorial roles within the BBC and commercial radio.

For decades, banks have managed emerging risks by extending existing frameworks. New regulations led to new controls. New technologies led to new governance processes. New market shocks led to revised stress tests.

Today, that approach is being seriously tested on a daily basis.

The convergence of geopolitical fragmentation and artificial intelligence is creating risks that evolve faster than many institutions can identify, escalate, and manage them.

More importantly, these forces are increasingly interacting with one another, creating a level of complexity that traditional governance structures were simply not designed to handle.

The greatest challenge facing risk leaders, then, is not simply geopolitical risk. Nor is it AI risk. It is the combination of the two.

The Bank for International Settlements (BIS) has warned that AI is increasing the complexity of the financial system itself. In a January 2026 speech on financial stability, the BIS noted that AI can make risks "more difficult to observe and assess" because of opaque models, unstructured data, and growing reliance on third-party providers.

Diverging sanctions regimes, technology restrictions, data localization requirements, and competing regulatory standards are creating a world in which global consistency is becoming increasingly difficult to achieve.

Recent analysis suggests that more than 70 countries are developing distinct AI-related regulatory frameworks, and in the process creating a patchwork of requirements that institutions must navigate simultaneously.

Artificial intelligence is accelerating these pressures.

"Artificial intelligence is transforming financial services faster than existing governance frameworks are evolving," said Sonia Baxendale, President and CEO of the Global Risk Institute.

She added that managing AI risk "is no longer confined to individual institutions" and increasingly requires coordination across the wider financial ecosystem.

Historically, risk management operated on relatively predictable timelines.

A threat emerged, specialists analyzed it, governance committees reviewed it, and management approved a response. Today, AI-enabled systems can generate decisions, identify vulnerabilities, or influence markets in near real time.

The International Monetary Fund recently warned that advanced AI models are dramatically reducing the time and cost required to discover and exploit vulnerabilities in critical systems.

According to the IMF, AI-driven cyber attacks could create “correlated failures” across multiple institutions because many banks rely on common software, cloud providers, and technology platforms.

This represents a fundamental shift in the nature of systemic risk. Traditional cyber attacks generally affected individual institutions. AI-enabled attacks have the potential to expose weaknesses across multiple organizations simultaneously.

> ***The greatest challenge facing risk leaders is not simply geopolitical risk. Nor is it AI risk. It is the combination of the two.***

As IMF Managing Director Kristalina Georgieva noted, AI is transforming finance while also fueling increasingly sophisticated cyber attacks that could trigger funding strains and broader market disruption.

Geopolitical shocks are now capable of changing regulatory expectations, sanctions requirements, supply chains, energy markets, and customer behavior almost overnight. AI amplifies the speed at which information moves through those systems.

A sanctions change announced in one jurisdiction can be analyzed, distributed, interpreted, and acted upon globally within minutes. While that creates opportunities for faster decision-making, it also increases the risk of errors, inconsistent responses, and governance failures.

Many institutions are already struggling to keep pace. Recent research among financial organizations found that 43% of large firms still lack AI-specific governance frameworks despite growing adoption.

But the deeper issue is that governance itself is becoming a bottleneck.

Many banking control frameworks were designed for a world where risks developed over weeks or months.

AI and geopolitical volatility are compressing those timelines into days or even hours. Traditional committee structures, escalation processes, and model validation approaches can struggle to respond at the required speed.

This explains why operational resilience has become a central focus for regulators globally.

Increasingly, supervisors are asking not whether institutions can predict every disruption, but whether they can continue operating when disruptions occur.

Risk managers must move beyond siloed approaches that treat technology, cyber, geopolitical, operational, and third-party risks separately and instead prioritize integrated risk frameworks built around resilience, scenario analysis, and rapid decision-making.

Boards must improve their understanding of emerging technologies. AI governance must be embedded into product development rather than applied retrospectively. Stress testing should increasingly focus on interconnected scenarios that occur simultaneously.

Institutions should also establish cross-functional crisis teams with the authority to act quickly when conditions change.

The most important shift, however, is cultural. Risk management can no longer assume that threats will emerge slowly enough for traditional governance cycles to keep pace.

CAREERS:

Optimism as a Career Strategy: The Story of Namit Sharma

Namit Sharma is the cofounder at XelerAIT Solutions. He is a risk management professional with more 25 years of experience, primarily in consulting and analytics for financial services, across consumer banking, capital markets, life and P&C insurance. He has extensive experience in credit, market, and operational risk.

Namit Sharma's career does not read as a steady climb up one ladder.

An alumnus of the Indian Institute of Management Calcutta, he has spent almost 3 decades as a leader inside the discipline of risk, moving through GE and Genpact, through Fidelity, and into catastrophe modeling at RMS, where he came to lead the analytics and data services function.

Four distinct kinds of risk, market, consumer credit, insurance, and catastrophe, in a single career. Ask him what connected the moves, and the answer is not ambition. It is optimism, and he insists it can be learned.

He begins by clearing away the usual vocabulary. Humility, curiosity, positivity: these fill every leadership book, and almost everyone, even the most difficult colleague, privately believes they possess them.
They are the surface. The real test, Sharma argues, comes where the rubber meets the road, at the moment theory has to produce a result and the outcome is genuinely uncertain.

The quality that shows up there is optimism, and it asks far more than cheerfulness. It is a willingness to loosen your grip on control, to empower other people, and to accept that the result is then no longer entirely yours to dictate.
A leader unwilling to give up that control cannot be optimistic in any way that counts.

Optimism of that kind is not summoned by force of will; it is fed by evidence.

It grows when people watch ideas combine with another and produce something no single idea could have reached alone, when two and two visibly begin to make five. Results build momentum, momentum builds confidence, and confidence is the raw material of optimism.

This is why Sharma is so deliberate about who is on a team. He looks for differentiated, complementary skills rather than reflections of his strengths, and trusts by default, because secure, talented people are not threatened by the talent around them.

Their collaboration adds rather than competes.

His path is the working example. Each move, from market risk into consumer credit, then into insurance, then into catastrophe risk, posed the same choice: treat unfamiliar ground as a threat, or as another place to learn and contribute.

He chose the second reading every time. None of these were reckless leaps; Sharma is a planner who controls the variables he can and keeps a fallback ready.

But by visibly taking calibrated risks himself, he earned the standing to ask others to do the same. A leader who can point to that kind of track record is believed when he says a hard thing is possible.

The harder task, he says, is making optimism collective rather than personal. A leader can be privately hopeful and still preside over an anxious team.

What lifts a whole group is the ability to paint a larger picture, held loosely enough that the team can reshape it, and resting on what he calls the invisibles: integrity, fairness, openness, simply being a good colleague. None of this, he stresses, is innate.

Pressed on whether someone early in their career could build the same optimism, he is specific: think in a longer time horizon, so a single bad week does not deflate you; build self-trust first, since you cannot extend real confidence to others until you are secure in yourself; and stay open to more than one version of success.

There is a discipline beneath the optimism that keeps it from tipping into wishful thinking. Sharma has a planner's instinct for looking around corners, for anticipating both the opportunity and the threat in whatever lies ahead.

His optimism is not blind; it is paired with that foresight, which is exactly what makes it safe for others to share.

His career, read closely, is less a record of where he went than an argument for how anyone might travel. Optimism is the engine, and it can be built.

UNVEILING THE HIDDEN AI

FAILURES BEYOND THE HYPE

Naresh Raheja is a Senior Risk Specialist & Examiner at the Office of the Chief National Bank Examiner. He has previously held senior data analytics roles at One Concern, ScoreData Corp and Fairfax Financial Holdings Limited, among others.

Artificial intelligence systems may appear highly capable, articulate and sophisticated, but many still fail in ways that create profound operational, compliance and governance risks for financial institutions, according to Naresh Raheja.

Raheja, Senior Risk Specialist & Examiner at the Office of the Chief National Bank Examiner, argues that banks are now entering a critical phase where AI risk shifts from experimental technology concerns into core operating-model risk.

And as generative AI tools become embedded within customer service, documentation, risk analysis and decision-making workflows, this transition is set to accelerate exponentially..

"AI capability does not guarantee AI reliability," Raheja says.

Drawing on lessons from failures across industries including airlines, healthcare, legal services, retail and media, Raheja outlines ten major dimensions of AI risk that banks must now confront. Those include hallucinations, algorithmic bias, instability, misinformation, data leakage, automation bias and failures involving human oversight.

He warns that AI systems frequently perform impressively in controlled demonstrations but become unreliable once exposed to complex real-world environments, edge cases and changing operating conditions.

"Modern AI systems can appear very capable but may suffer from reliability issues," he writes in a self-published paper on the subject. "They may be articulate, knowledgeable, and persuasive, yet they can sometimes fail in ways that matter when deployed in real-world environments."

Among the examples highlighted by Raheja is the Air Canada chatbot dispute in which a customer receives incorrect bereavement fare information from an AI assistant and the airline is later held responsible for the chatbot's inaccurate guidance.

Another case involves a UK parcel delivery chatbot manipulated into insulting its own employer publicly.

For banks, Raheja believes such failures carry significant implications because customer-facing AI systems increasingly influence financial decisions involving payments, lending, hardship support, collections and product eligibility.

AI capability does not guarantee AI reliability.

"This creates potential risks for consumer protection, UDAAP, complaint management, mis-selling, and legal liability," he says.

Raheja also expresses concern about "hallucinations" where AI systems generate convincing but false information.

He points to legal cases involving fabricated court citations and AI-generated finance articles containing inaccurate financial explanations as examples of how persuasive but unreliable outputs evade human scrutiny.

"The banking analog is not only a hallucinated customer answer, but also a hallucinated control narrative, policy interpretation, credit memo, model validation summary, board report, or regulatory response that appears polished enough to pass review," he warns.

Another major issue identified by Raheja is algorithmic bias. He notes that AI systems trained on historical data can unintentionally reproduce discriminatory patterns, potentially exposing banks to fair lending violations, reputational damage and regulatory scrutiny.

At the same time, he cautions that AI models often struggle with "brittleness" and instability. Systems that appear highly accurate during development may degrade rapidly once operating conditions shift or data patterns evolve.

He references the collapse of Zillow's automated home-buying program and healthcare AI systems that fail under real-world conditions despite strong testing performance.

"Models and GenAI-enabled workflows used in financial services may perform well during validation but fail when economic conditions shift, new data patterns emerge, customer behavior changes, policies are updated, or the system is exposed to real operational exceptions," he writes.

Raheja additionally warns against excessive trust in AI-generated outputs. He describes automation bias as one of the most underestimated risks facing organizations adopting generative AI technologies.

"A 'human-in-the-loop' is only effective if the human has sufficient expertise, time, authority, incentives, and evidence to challenge the output," he claims. "Otherwise, human review can become a rubber stamp."

Data leakage, too, remains a growing concern. Raheja highlights incidents where employees enter confidential information into public AI systems, potentially exposing sensitive institutional data and proprietary information.

Beyond the technical risks, Raheja believes explainability and governance may become some of the most difficult challenges for banks. Regulators increasingly expect institutions to explain AI-driven decisions involving lending, compliance, collections and customer servicing.

"When AI systems influence credit, risk, compliance, servicing, collections, or regulatory decisions, banks must be able to document not only the 'why' behind an output, but also the evidence used, the policy basis for the decision, the human review performed, and any escalation or override," he writes.

The lesson here is that banks should treat AI failures across other industries as advance warning signs rather than irrelevant incidents. Institutions capable of translating those lessons into practical controls before AI becomes deeply embedded into critical workflows may ultimately prove more resilient than competitors focused solely on speed of adoption.

CLOSING THE SIGNAL GAP

Lessons From Risk Evolve London on the Future of Risk Decisioning

Lisa Kalscheur is Chief Marketing Officer at Weave.AI and a veteran technology marketing leader with senior roles across multiple high-growth AI, SaaS and digital platform companies.

During the Non-Financial Risk (NFR), Operational Risk and Resilience track at CefPro Risk Evolve London 2026, one theme surfaced consistently across every session:

Financial institutions are not short on data.

The bigger challenge is identifying, interpreting, and acting on the right signals in time. Increasingly, it's not just about reacting to signals - it's about knowing what you're missing in the first place: uncovering the "unknown unknowns."

Across discussions on AI, cyber resilience, third-party risk, operational risk, RCSA, and culture, a clear picture emerged. The industry is drowning in data, but struggling to identify the right signal - or sometimes the lack of signal - early enough to get ahead of risk.

This is the problem of decision latency: the gap between identifying what matters and acting on it. It is rapidly becoming one of the defining challenges for today's CROs.

This is also where the concept of "decisioning" is emerging - not decision-making as a point-in-time activity, but a continuous capability to detect, interpret, and act on signals in real time.

One message came through clearly across the conference: risk has become exponentially more interconnected, complex, and fast-moving.

Cyber risk, operational risk, geopolitical instability, third-party exposure, AI adoption, and reputational threats no longer exist in isolation. Risks now compound across domains, often faster than organizations can respond.

As Dr. Suren Pakhchanyan, Chief Risk Officer at Inecobank, noted in his keynote, risk teams are now

dealing with “thousands of risk events every month,” much of it buried in unstructured data. More critically, many risks sit beyond the reach of observable data altogether - blind spots across fourth- and fifth-party dependencies, or situations where the absence of signal is itself meaningful.

These blind spots fundamentally change how risk must be understood - where silence is no longer comfort, but ambiguity.

In response, firms are increasingly turning to AI to help surface what traditional approaches miss. Multiple panelists discussed how AI is beginning to transform risk management through anomaly detection, cyber monitoring, and continuous analysis of unstructured data.

Chhavi Kakkar of NatWest emphasized that agentic AI must work within the pace and realities of the first line to become truly valuable for RCSAs and operational risk workflows.

> ***“We’re looking outside the four walls more than ever because that’s often where the first signal shows up.***

Pakhchanyan also shared an example where AI improved risk categorization accuracy from 67% to 92% while cutting reporting time in half.

But the real opportunity is not simply faster reporting. It is faster, more confident decisioning - especially in environments where signals are incomplete or fragmented.

The conference also highlighted how quickly risks now amplify across domains. Discussions featuring Nassos Economopoulos (Rothesay), Fraser Hughes (NatWest), and Mihaela Breg (Europe Arab Bank) highlighted how cyber, operational, geopolitical, and third-party risks are increasingly converging.

As organizations become more digitally connected and operationally complex, risk leaders are increasingly focused on understanding how signals connect - and how quickly they compound.

This shift is also forcing organizations to rethink traditional Risk and Control Self-Assessments (RCSAs). Multiple panelists acknowledged that RCSAs are often treated as static compliance exercises rather than dynamic decision tools.

One panelist described RCSAs as “mostly a compliance exercise” completed annually. That approach creates a dangerous illusion of control, where completion is mistaken for coverage, and documentation is mistaken for decision readiness.

The shift we heard repeatedly throughout the event was clear: RCSA frameworks must evolve into living systems that continuously adapt to real-time signals, changing exposures, and emerging threats.

At the same time, another underlying theme emerged consistently across sessions: the growing importance of external context.

Internal data explains what has already happened. External signals often indicate what is emerging - and what institutions may be missing entirely. Panelists repeatedly emphasized the need for continuous monitoring of peer activity, regulatory developments, market sentiment, and broader ecosystem dependencies.

Lisa Migheli of MUFG reinforced that third-party risk can no longer be managed in isolation, requiring continuous external monitoring and deeper visibility into fourth- and fifth-party dependencies.

As one speaker noted, “We’re looking outside the four walls more than ever because that’s often where the first signal shows up.”

This reflects a broader shift in risk management: from documenting known risks to continuously identifying hidden vulnerabilities and emerging exposures before they become material events.

Ultimately, the conference reinforced that the CRO role itself is evolving. As Sean Titley, Chief Risk Officer at Bank of London, emphasized, the CRO is shifting from oversight and reporting toward enterprise-wide decision leadership under uncertainty.

Today’s risk leaders are increasingly responsible for:

- Uncovering blind spots across the organization and ecosystem
- Connecting signals across silos
- Prioritizing action in real time
- Balancing speed with defensibility and control

The CRO is no longer just asking, “Are we compliant?”

They are increasingly asking, “Are we making the right decisions, fast enough?”

In a risk landscape defined by speed, complexity, and ambiguity, the advantage will go to institutions that can identify what matters, understand what is missing, and turn signals into decisions before risk becomes consequence.

TRENDWATCH:

BANKING'S NEXT CRISIS MAY BE HIDING OUTSIDE THE BANKING SYSTEM

> *Senior risk managers increasingly worry that hidden leverage could trigger contagion before regulators fully detect it.*

For senior risk managers across global banking and financial services, concern is increasingly shifting away from traditional balance sheet threats toward a far more complex and opaque challenge - the growing interconnectedness between banks, private credit markets and non-bank financial institutions.

What began as a post-financial-crisis migration of lending activity away from heavily regulated banks has evolved into a vast ecosystem of private lenders, securitized exposures, leveraged financing arrangements and shadow banking structures that many regulators fear are only partially understood.

As defaults rise, liquidity tightens and geopolitical instability intensifies, risk leaders are increasingly focused on whether hidden leverage, weak transparency and indirect exposures could trigger contagion effects capable of spreading faster than institutions or regulators can fully detect.

01

Source: Financial Stability Board

PRIVATE CREDIT MARKETS NOW EXCEED $3 TRILLION GLOBALLY

The global private credit market has expanded dramatically since the 2008 financial crisis as tighter regulation pushed riskier lending activity away from traditional banks. The Financial Stability Board estimates suggest the market now exceeds $3 trillion globally, making it one of the fastest-growing areas of modern finance. Risk managers increasingly worry that rapid growth, weaker transparency and inconsistent reporting standards may be masking hidden leverage and deteriorating underwriting quality across parts of the sector.

02

Source: Bank of England

95% OF FINANCIAL STABILITY EXPERTS CITE GEOPOLITICAL RISK AS A MAJOR THREAT

The Bank of England's latest Systemic Risk Survey found that 95% of respondents view geopolitical risk as a major threat to financial stability. Unlike traditional economic shocks, geopolitical tensions now affect sanctions compliance, energy markets, supply chains, liquidity conditions, operational resilience and cyber exposure simultaneously. Senior banking risk leaders increasingly describe geopolitics not as a standalone risk category, but as a multiplier capable of intensifying virtually every other major financial and operational threat.

03

BANKS HOLD HUNDREDS OF BILLIONS IN INDIRECT PRIVATE CREDIT EXPOSURE

Although private credit lending often sits outside traditional banking structures, banks remain deeply connected to the sector through warehouse financing, leverage facilities, securitization structures and fund partnerships. According to Reuters, regulators increasingly fear that institutions may not fully understand the scale of their indirect exposure. Recent losses involving lenders such as Market Financial Solutions have intensified scrutiny around how private credit risks could spread back into regulated banking systems during stressed market conditions.

Source - Reuters

04

MORE THAN HALF OF BUSINESS DEVELOPMENT COMPANIES TRADE BELOW ASSET VALUE

A growing number of publicly traded business development companies now trade at significant discounts to their reported net asset values. Per The Wall Street Journal, Investors increasingly view those discounts as warning signs that underlying loan valuations may not fully reflect deteriorating credit conditions. For risk managers, the concern is less about individual firms and more about whether wider private market pricing remains artificially stable because many assets are not subject to continuous public market valuation.

Source - The Wall Street Journal

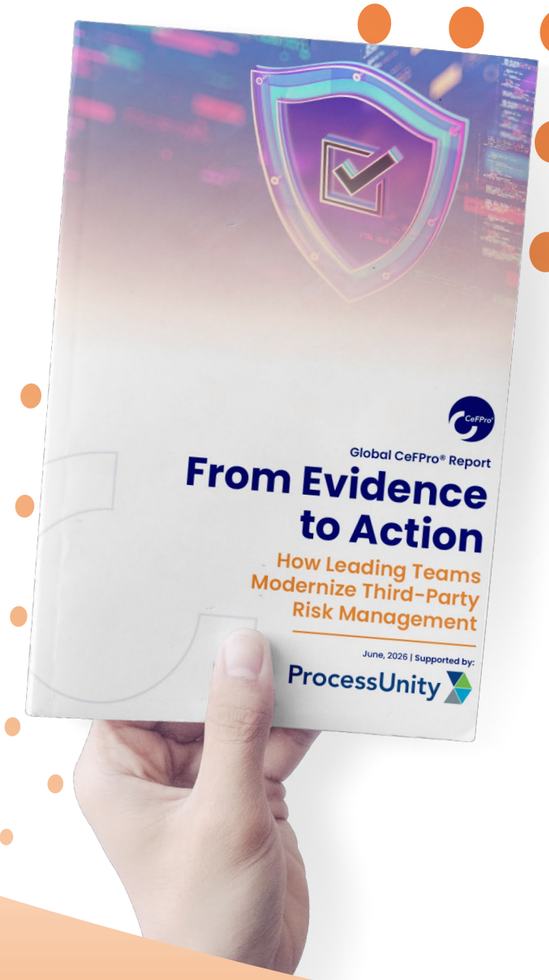
05

OPERATIONAL RESILIENCE HAS BECOME AS IMPORTANT AS CAPITAL RESILIENCE

Regulators globally are placing growing emphasis on operational resilience rather than focusing solely on capital and liquidity strength. The Bank for International Settlements (BIS) says senior risk managers now face increasing pressure to demonstrate that institutions can continue operating during cyber incidents, supplier failures, geopolitical disruptions or third-party outages. The shift reflects broader recognition that modern banking crises may emerge from operational breakdowns, interconnected dependencies or infrastructure failures rather than traditional credit losses alone.

Source - The Bank for International Settlements

"More than a third of institutions still manually map vendor evidence to security controls using spreadsheets or documents.



FROM EVIDENCE TO ACTION

Why are today's third-party risk assessments holding teams back?

Assessment fatigue is real. New research sponsored by Process Unity reveals where TPRM breaks down.

ProcessUnity

Want to conduct your own research?
Get to the heart of the issues that matter, access the audiences you need, and uncover robust insights that power content, thought leadership, and demand generation.
Find out more at: cefpro.com/market_research

Download the full research report for free here ›

INTRODUCING ISO37008:

The role it plays in governing investigative compliance

Simon Scales is Chief Education & Development Officer at the Association of Corporate Investigators. He has previously held senior investigative and regulatory positions within, among others, the Lloyds Banking Group, The Pensions Regulator, and BP.

ISO 37008 is an International Standards Organisation (ISO) guidance document that sets out a framework for how organisations should design, govern and conduct internal investigations.

Published in July 2023, it sits within the broader ISO 37000 series on organisational governance and integrity, alongside guidance on governance, anti-bribery management systems, whistleblowing, fraud control and governance maturity.

Whilst ISO 37008 is not a certifiable standard, it offers a practical, internationally informed reference point that strengthens how organisations manage investigative risk. Investigations are a natural extension of effective governance and a necessary complement to compliance programmes.

Compliance management focuses on what should happen; investigations establish facts about what did happen when governance or controls fail.

Used together, ISO 37002 and ISO 37008 reinforce a strong risk, control and governance environment and support the three lines of defence model.

The document defines an internal investigation as a professional fact-finding process initiated by an organisation to establish facts about suspected wrongdoing, misconduct or non-compliance.

Examples include bribery and corruption, fraud, bullying and harassment, violence, discrimination and breaches of a code of conduct. It also notes that the term “investigation” covers matters ranging from operational enquiries to serious misconduct issues, making clarity in governance documents essential.

ISO 37008 emphasises clear investigative governance, starting with a written investigations policy or procedure. In practice, organisations usually require both.

The guidance frames governance through practical questions covering where investigations sit within the organisation, accountability at executive and board level, outsourcing arrangements, reporting lines, regulatory requirements, triage and referral processes, oversight committees, management information, and whether investigators are suitably qualified.

The Association of Corporate Investigators (ACi) recommends governance artefacts that align with existing frameworks rather than replace them.

These include a charter defining the investigations mandate, an investigations policy covering remit and case allocation, procedures manuals, oversight committee terms of reference, investigation response plans for significant cases, and templates supporting planning, investigative actions and reporting.

The overall objective is consistency, transparency and defensible decision-making, particularly where multiple functions interact during investigations.

The ACi also recognises that many organisations locate investigations within Audit or Legal reporting lines, while some combine investigations and whistleblowing within a wider Business Integrity function.

A central feature of ISO 37008 is its articulation of investigation principles. Five key principles are identified: investigations should be independent, confidential, competent and professional, objective and impartial, and legal and lawful.

The guidance also formalises an end-to-end investigation lifecycle covering allegation assessment, planning, evidence collection, interviews, reporting and closure. This codifies what “good” looks like and embeds decisions and actions within a defensible framework.

> ***Compliance management focuses on what should happen; investigations establish facts about what did happen when governance or controls fail.***

The guidance also addresses enabling support for investigations, including personnel, funding, technical tools and organisational infrastructure sourced internally or externally.

It highlights technology as an efficiency driver, particularly data mining, advanced search, e-discovery and AI capabilities that improve speed, accuracy and scalability.

Whether organisations invest in investigative technology depends on organisational size and case volumes, but mature investigative functions increasingly rely on technology to reduce dependency on third parties and standardise practice.

At the same time, external providers such as law firms, consultancies and forensic specialists continue to play an important role, particularly where legal privilege, litigation, self-reporting or regulatory cooperation is involved.

ISO 37008 also focuses on the human impacts of investigations. It addresses protection, safeguarding and anti-retaliation measures for everyone involved, particularly whistleblowers who may be legally protected in many jurisdictions.

Organisations are encouraged to foster a speak-up culture supported by tone from the top, accessible reporting routes and formal whistleblowing channels.

Investigators should be protected from undue influence, supported by senior leadership and able to operate without fear or favour.

Finally, investigations should generate control improvements and thematic learning. ISO 37008 emphasises the value of identifying control weaknesses and implementing remedial actions promptly rather than waiting for investigations to conclude.

Effective stakeholder engagement is also essential. Large organisations often operate in silos, yet successful investigations require coordinated communication across functions and levels. Investigation response plans can help structure stakeholder management and decision-making.

On the question of centralisation, ISO 37008 recognises that investigations are not one-size-fits-all because different case types demand different specialist skills. However, the ACi advocates a centralised investigations team to support specialists, drive consistency, concentrate expertise and strengthen quality assurance and training.

The ACi view is that Compliance should combine independence with direct visibility to senior leadership while maintaining strong relationships with Legal and Risk.

ONSTAGE

Key Voices to Hear

Next Gen OpRisk Europe

October 13-14, 2026 | London

Technology is **evolving.** Risk is **intensifying.** Operational resilience is **non-negotiable.**

Join senior experts and industry leaders to explore how organisations are reshaping operational risk frameworks in response to **AI adoption, escalating cyber threats, and complex technology dependencies.**

Discover how firms are **integrating risk across functions,** embedding **technology risk into governance,** and strengthening **enterprise-wide resilience.**

Walk away with **practical approaches** to:

- Strengthen operational resilience as a strategic capability
- Improve decision-making through better data and AI oversight
- Navigate an increasingly complex and fast-moving risk landscape

Stand Out Speakers

Find Out More >

Are you interested in attending?

View full agenda here

View full speaker line-up here

Register your place here

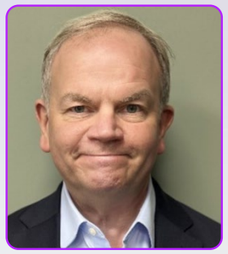
Rajeev Bhatnagar
Chief Risk & Compliance Officer
BNY

Koen Harmsen
Head of Non-Financial Risk Management
ING

Nitesh Kumar
Managing Director – Global Head of Cyber, Payment Systems Risk and Strategic Projects
BNP Paribas

Violeta Cadosch
Head of Operational Resilience & Governance L&H Reinsurance
Swiss Re

Prash Patel
Managing Director – Head of Operational Risk
Barclays CIB



Sean Titley
Chief Risk Officer
Bank of London

Ben Jeary
Head of Operational Risk
Santander

Kishan Majithia
Executive Director – Cyber & Technology Controls
J.P. Morgan Chase & Co

Karim Sultan
Head of Operational Technology and Cyber Risk
Standard Chartered Bank

Andrew Pym
Head of Operational Resilience
Monzo

View full speaker line-up here >

THE REASON RISK CULTURE FAILS WHERE INCENTIVES WIN

David Buck is Head of Enterprise Risk Management at T. Price Rowe. He has previously held very senior risk and finance management roles with insurance giant USAA and Citizens Financial Group.

Financial institutions may have spent years refining governance structures, risk frameworks, and oversight controls, but many organizations still struggle to embed risk culture into everyday decision-making where it matters most.

That is the view of David Buck, Head of Enterprise Risk Management at T. Rowe Price, who argues that risk culture only becomes effective when it moves beyond reporting exercises and becomes embedded in the operating rhythm of a business.

"The shift happens when risk stops being something you report on and starts being something you actually do," Buck said. "The organizations that get this right integrate risk into their existing operating rhythm — their planning cycles, their business forums, their deal approvals — rather than only standing up separate risk committees that run in parallel to the business."

Buck believes one of the strongest indicators of a healthy risk culture is when executives openly challenge assumptions and discuss uncertainty as part of routine decision-making rather than treating risk as a separate governance activity.

"When you hear senior executives ask 'what are we trading off here?' or 'what could we be wrong about?', it signals that uncertainty is a legitimate part of the conversation," he said.

> ***Risk appetite becomes a source of competitive advantage rather than a compliance artifact.***

Drawing on behavioral economics, Buck argued that organizations should focus on designing processes that naturally encourage risk-aware decisions instead of relying solely on mandates or compliance structures.

"The concept of choice architecture suggests that if you design decision processes so that risk-aware choices are the default, you don't have to mandate good behavior," he said. "You just make it easier."

Buck also warned that many institutions continue to struggle when translating board-level risk appetite statements into operationally meaningful metrics.

"The core discipline is cascading architecture," he explained. "Taking enterprise-level appetite statements, focusing on the most impactful risks, and translating them into specific tolerances with defined thresholds, owners, and escalation triggers."

However, Buck cautioned that firms frequently fall into the trap of excessive measurement, creating dashboards so overloaded with indicators that they generate a false sense of control.

"A dashboard with hundreds of metrics that no one acts on is arguably worse than no dashboard at all," he said, "because it creates the illusion of oversight."

According to Buck, organizations that are most effective at embedding risk appetite directly connect risk indicators to business planning and resource allocation decisions rather than treating them as governance exercises reviewed once a year.

He also stressed that policies alone are insufficient to influence behavior unless employees find them practical and relevant to daily work.

"What truly drives behavior is whether people find policies clear, relevant, and consequential in their day-to-day work," Buck said.

That means firms must communicate risk expectations consistently through practical examples, narratives, and decision-making guidance rather than depending entirely on formal attestations.

Buck added that institutions should focus far more heavily on behavioral indicators such as escalation frequency, audit findings, and near-miss reporting rather than simply measuring policy acknowledgments.

On incentives, Buck argued that many compensation structures unintentionally encourage behavior that conflicts with stated risk appetite because they reward outcomes rather than how those outcomes are achieved.

"If a business unit hits its revenue number by taking on concentrated exposure that violates risk appetite, the P&L still looks good," he said.

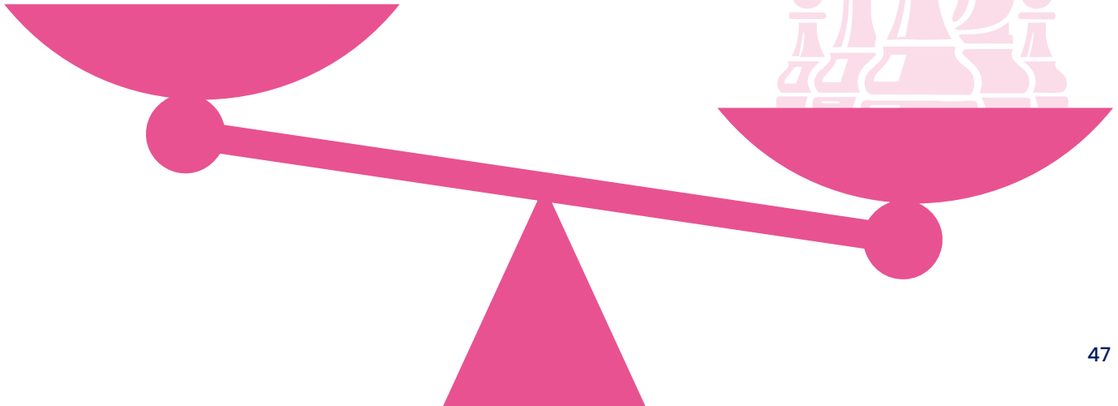
He believes compensation committees should incorporate risk-adjusted performance metrics, conduct indicators, and risk utilization measures directly into executive scorecards.

"The most powerful lever is cultural," Buck said. "When a leader visibly rewards a risk-aware decision that gave up short-term gain, or when a clawback decision explicitly references a risk culture failure, it makes the stakes real."

Buck also sees major potential for artificial intelligence and advanced analytics to reshape how firms monitor risk culture in real time.

"We're at an inflection point where risk culture is starting to move from a lagging, survey-based discipline toward something closer to real-time sensing," he said.

Technologies such as natural language processing may help firms identify early signs of cultural drift, suppressed dissent, or inconsistent governance behavior across business units.



At the same time, Buck warned that firms must carefully balance cultural measurement with employee privacy and ethical governance.

"These tools need rigorous oversight," he said. "Organizations need to draw a clear line between measuring risk culture and surveilling employees."

Looking ahead, Buck believes risk appetite frameworks themselves must evolve to remain relevant in an environment shaped by persistent volatility, geopolitical shocks, and rapid structural change.

"In a world of persistent shocks and structural change, a static, once-a-year risk appetite exercise is no longer effective," he said.

Instead, he advocates for scenario-aware, data-driven approaches that allow firms to adapt exposures and decision-making dynamically as conditions change.

"If done well," Buck said, "risk appetite becomes a source of competitive advantage rather than a compliance artifact."

Upcoming CeFPro Events

North America

Vendor & Third Party Risk USA: The Cross Industry Conference
October 14-15 | Fort Worth

Funds Transfer Pricing Workshop
October 26 | Charlotte

Balance Sheet Management USA
October 27-28 | Charlotte

Next Gen OpRisk USA
November 3-4 | New York City

AI Governance USA
November, TBC | New York City

EMEA

Balance Sheet Management Europe
September 22-23 | London

Next Gen OpRisk Europe
October 13-14 | London

Climate Risk Europe
October 20-21 | Amsterdam

Vendor & Third Party Risk Europe: The Cross Industry Conference
November 10-11 | London

AI Governance Europe
December 1-2 | London

View our full upcoming events calendar at **www.cefpro.com/forthcoming-events**