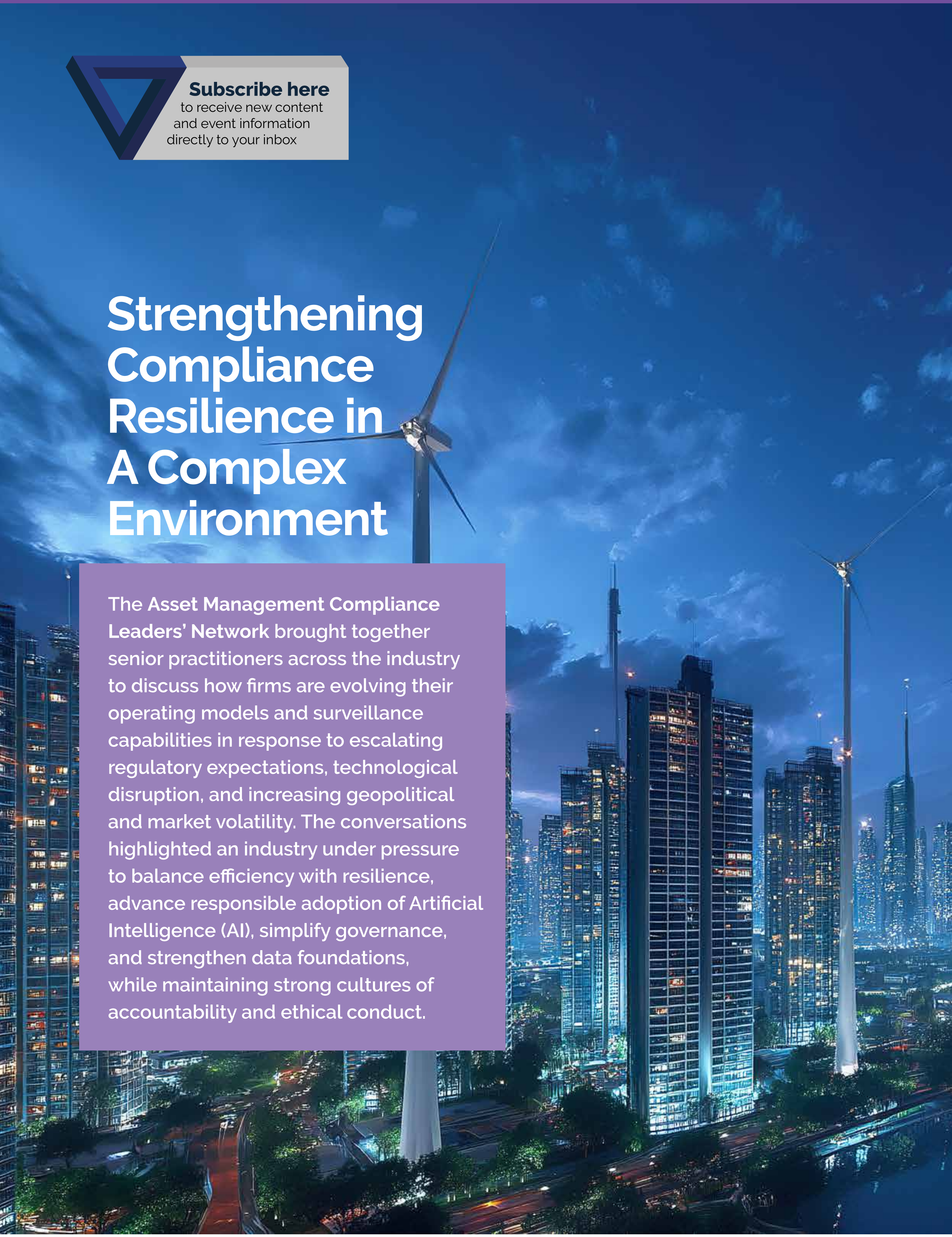
A 1LoD report

Asset Management Compliance
LEADERS' NETWORK

FORECAST 2025

Strengthening Compliance Resilience in A Complex Environment

Sponsored by ACA® BEHAVOX



Subscribe here
to receive new content
and event information
directly to your inbox

Strengthening Compliance Resilience in A Complex Environment

The **Asset Management Compliance Leaders' Network** brought together senior practitioners across the industry to discuss how firms are evolving their operating models and surveillance capabilities in response to escalating regulatory expectations, technological disruption, and increasing geopolitical and market volatility. The conversations highlighted an industry under pressure to balance efficiency with resilience, advance responsible adoption of Artificial Intelligence (AI), simplify governance, and strengthen data foundations, while maintaining strong cultures of accountability and ethical conduct.

Key takeaways

1. Firms are shifting from expansion to efficiency however ineffective governance continues to slow decision-making

2. Adoption of AI and automation remains cautious, with benefits still outweighed by reliability concerns

3. Data quality is the biggest barrier currently to progress in both surveillance and integrated non-financial risk management

4. Surveillance frameworks are expanding but remain fragmented and heavily rules based

5. Culture and accountability remain the strongest determinants of effective risk management

Subscribe here
to receive new content
and event information
directly to your inbox

"I really appreciate the thoughtful insights and dialogue 1LoD roundtables inspire."

ROGER TRIMBLE, HEAD OF TRADE SURVEILLANCE AND COMPLIANCE MONITORING, MORGAN STANLEY WEALTH MANAGEMENT

Enhancing Risk and Control Operating Models in a Tighter, Faster Environment

Pressure on cost and speed has driven much of the recent evolution in firms' risk and control operating models. For years, teams were asked to "do more with less," and the strain of this expectation is now visible. Budgets have tightened, risk appetites have become more conservative, and yet expectations for efficiency continue to grow. One participant reflected that during earlier periods of expansion, firms invested heavily in the 3 lines of defence, but now there "is reduced capital investment and appetite to do so." The focus has shifted firmly to efficiency, with technology seen as the primary lever, although another noted that "while AI is creating efficiencies, you're actually creating a lot more work."

Technology, however, was not the only constraint in driving improvements. Many agreed that the current operating models were still too bureaucratic and slow to support agile, investment-led decision making. One participant noted firms had created "over-governance", with layers of committees and reviews that often delayed action. This was especially difficult for front office teams under pressure to move quickly. As one participant observed, committee structures designed to enhance oversight had ended up "stopping progress" instead. Several firms were now collapsing or consolidating committees, identifying true decision-making bodies, and striving to "right-size" governance so that it enabled, rather than obstructed, the business.

Alongside simplification, there was a clear push to embed emerging risks more visibly into frameworks. One participant described how their firm was integrating geopolitical risk as a distinct risk stripe, reporting it to the board alongside operational and compliance risk. Another said their firm viewed geopolitical events not just through sanctions compliance but also reputational and investment exposure, showing how non-financial risks were converging. These examples reflected a broader trend where firms were embedding resilience and anticipation directly into their control frameworks, aiming to respond faster when market or political conditions shifted.

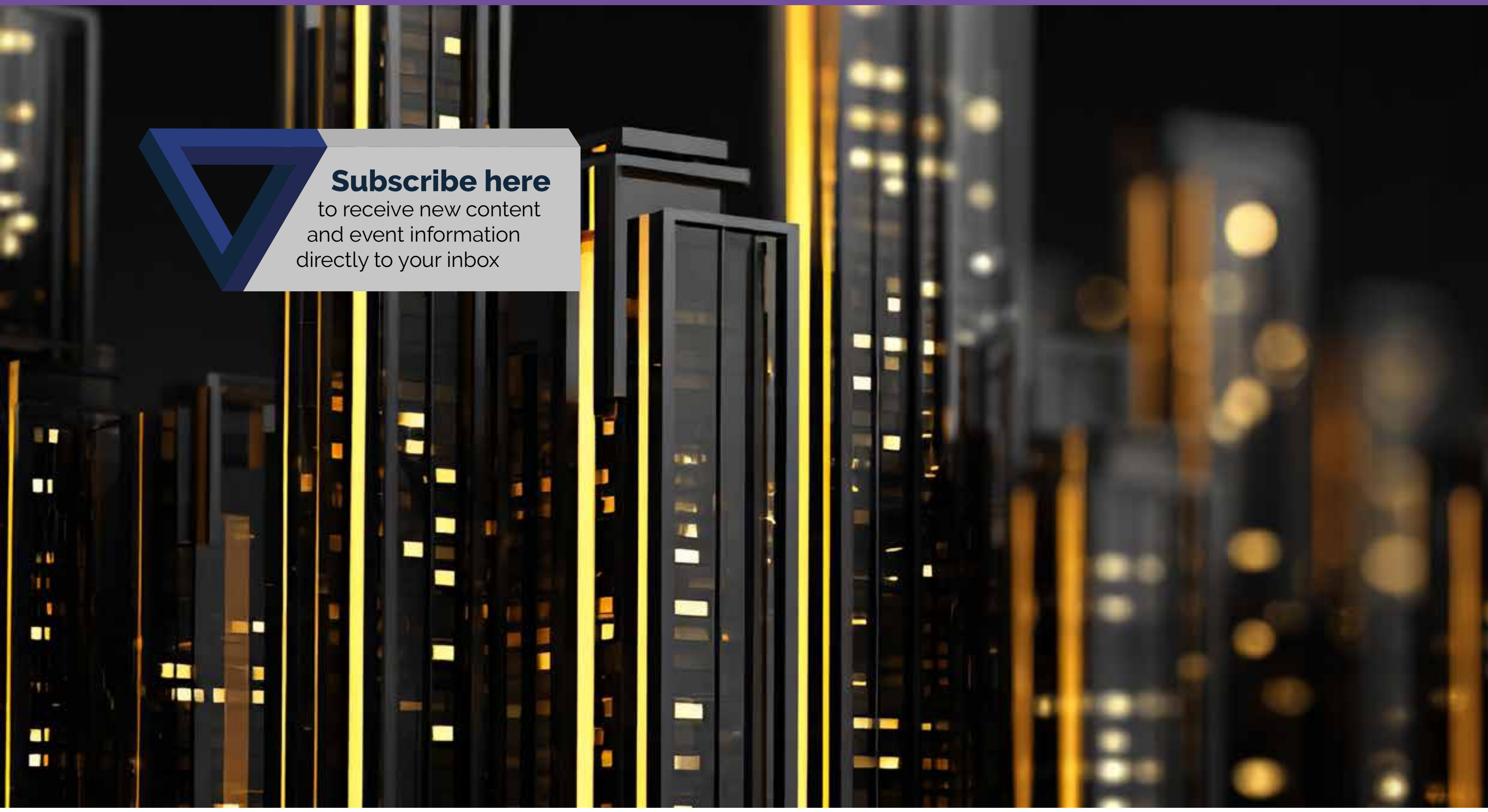
Leadership and accountability also formed a central thread. There was widespread recognition that risk ownership has to sit firmly within the business, not with compliance or risk functions. One participant noted their firm had introduced a simple but effective mechanism: every business leader's annual performance review included feedback from at least one control partner. They confirmed this helped reinforce the "culture of ownership" and reminded leaders that good control was integral to performance. Others spoke of assigning dedicated compliance or risk staff to product teams so that control input began "as soon as an idea starts", stated one practitioner, rather than at the end of a process. These early engagements helped surface potential issues before they became blockers. Several participants noted that encouraging challenge culture was equally important, with one stating this helped in creating an environment where the business "liked being challenged" and saw value in explaining and defending its decisions.

Technology was, naturally, a recurring topic throughout. Most firms had begun experimenting with AI technologies, but experiences were mixed. Many found these technologies unreliable, producing incorrect or inconsistent outputs, especially in legal or regulatory contexts where precision was essential. "We end up doing double work," one participant said, "checking that the AI hasn't got something wrong." Others pointed out that tools designed to improve efficiency could, paradoxically, increase workloads as staff verified and corrected outputs. Despite this, there was optimism about their future potential. Internal chatbots had been built to provide quick advisory responses, while some firms were testing AI for shareholder disclosure and third-party due diligence processes. Still, all emphasised that there must be a human in the loop and that firms must never rely on AI-generated data in regulatory reporting without verification.

Education was highlighted as one of the biggest enablers of safe adoption, with one participant explaining the biggest challenge was not technology itself but a lack of understanding. Firms were focusing on equipping their staff, especially control and model risk teams, with the skills to assess AI systems properly. This educational investment was costly but seen as essential to long-term success. Others believed AI costs would eventually fall and become more commoditised, but one emphasised that in the short term, "maintenance and data quality are the real expense."

The conversation also turned to how firms were strengthening data governance to support technology deployment. Data completeness, accuracy and explainability remained persistent challenges, particularly as AI introduced "black box" outputs that could not be easily justified to regulators. Participants stressed that control functions must maintain oversight of model inputs, continuously test data integrity, and document decision logic to meet regulatory expectations.

Several participants described a shift towards proactive and anticipatory approaches, with one emphasising "getting ahead rather than reacting." Post-mortems were being run after major deals or strategic changes to identify communication gaps and improve coordination. Others spoke about embedding continuous dialogue between compliance and leadership to ensure early visibility of strategic initiatives. Emerging risks such as merger and acquisition (M&A) integration, private investment growth, cyber threats, and expanding books and records obligations were also front of mind.



The Next Evolution of Conduct Surveillance from Detection to Prevention

Participants agreed that the scope of communications surveillance has expanded significantly, but maturity levels vary widely across firms. Most monitor trade and electronic communications, while voice surveillance remains costly and produces high levels of noise. Several firms operate multiple systems, combining vendor with in-house solutions, yet many acknowledged that these systems still operate in silos, hindering integrated risk assessment. One firm, following an audit, "launched an entire surveillance department," illustrating the scale of uplift still underway across the industry.

Despite this progress, participants admitted that current frameworks were not fully fit for purpose. Rules-based models still dominated, despite years of discussion about risk-based approaches (RBAs), particularly in the United States, and high false-positive rates continued to sap resources. To support this, AI and behavioural analytics were viewed as promising but still developing tools. One successful direction was training AI models to filter noise and assign confidence scores to alerts, distinguishing between false positives and meaningful risks such as market abuse or harassment. Firms using these technologies were seeing "more interesting results", stated one participant, as AI improved its ability to interpret coded language and context.

However, most participants said they were only at the beginning of this journey. One participant described behavioural analytics as the striving of "pulling trade, comms, and everything else together to create a picture," but admitted, "we're not close to it yet." Data quality was seen as the biggest barrier and therefore biggest priority as, without clean, complete inputs, any predictive system risked being misleading.

Others spoke about the potential for AI to uncover patterns in conduct, such as identifying employees at risk of misconduct through changes in behaviour or communication style, but this raised privacy and ethical concerns. Firms based in regions with strict labour laws, particularly Europe, faced limits on how deeply they could monitor staff behaviour. To utilise this in a responsible manner, "We have to be very careful about how we tap into certain data," one participant explained.

If AI was the long-term hope, robust data governance was the immediate necessity to make surveillance more effective. Several had consolidated surveillance

This information was taken from the Asset Management Compliance Leaders' Network event in New York, 9 October 2025.

"Very Informative to hear other colleagues express industry challenges"

STEPHEN PETRICK, MANAGING DIRECTOR, ADVISORY COMPLIANCE, BLACKROCK

"Interactive and informative industry discussions."

ARLENE KLEIN, HEAD OF GLOBAL COMPLIANCE, T. ROW PRICE

data into central warehouses and introduced quality controls to ensure every alert was dispositioned. This complete data set allowed for better model training and trend analysis. One participant described how their organisation had begun correlating surveillance alerts with information including security logs and print activity to detect potential insider risks.

Efficiency gains were most evident when firms integrated trade and e-comms surveillance into a single workflow. This allowed investigators to move from a trade anomaly to all related communications "through one interface," improving both speed and depth of review, mentioned one participant. However, not all firms were ready to merge these functions. Some maintained clear separation, partly for confidentiality reasons, with security teams screening e-mails before escalating them to senior compliance or legal staff.

The strongest consensus emerged around culture. Participants agreed that surveillance alone could not change behaviour; it had to be supported by clear accountability frameworks, leadership engagement, and cultural reinforcement. Many firms had formalised accountability frameworks linking breaches to performance reviews and compensation. One described a "three-strike" escalation process culminating in human resource (HR) intervention; another tied persistent onboarding or know your customer (KYC) failures to direct financial penalties. These frameworks were viewed as essential to reinforce behavioural expectations. Yet several participants warned that excessive focus on punishment risked creating fear rather than integrity.

Instead, firms were attempting to cultivate partnership. Compliance officers positioned themselves as advisors highlighting their role: "I'm here to keep you out of trouble", rather than enforcers. This subtle shift appeared to encourage earlier engagement and self-disclosure. Additionally, leadership development and mindfulness programmes were being introduced to strengthen emotional intelligence and improve how compliance messages were delivered. "It's about motivating people towards good behaviour, not just punishing bad," one participant stressed.

Proactively striving to create a surveillance culture that moved away from oppressive was therefore agreed on. Excessive monitoring, one argued, could "kill proactivity" and make employees more cautious and less innovative. The challenge, several argued, was finding equilibrium: enough monitoring to deter and detect misconduct, but not so much that it damaged morale or drove behaviour underground.

XLoD Global 2026

LONDON
30 & 1
June July

NEW YORK
24
September

SINGAPORE
21
October

XLoD Global is the leading event globally for non-financial risk and control leaders from across the 3 lines of defence from banks and other financial institutions

SAVE THE DATE

XLoD Global
An in-person conference

www.1lod.com

CONFERENCE & EVENTS AWARDS 2025

"A stand-out event delivering impressive growth, commercial success, and exceptional value for its community."
Conference & Events Awards 2025

WINNER
EVENT OF THE YEAR
(UP TO 1200 ATTENDEES)
XLoD Global

Co-located with Risk Live and TDFM

1LoD