XLoD® Global

LONDON

Navigating the Future of Non-Financial Risk and Control:

Insights from XLoD Global - London

Lead Sponsor*

smarsh®

*Bespoke version created for Smarsh

XLoD Global
LONDON
13 & 14 Nov 2024

Lead Sponsors

acin
Bloomberg
Deloitte.
EVENTUS
IOX MARKETS
Nasdaq
NICE Actimize
ONETICK
smarsh
SteelEye

Co-Sponsors

BEHAVOX
Fenics MarketData
Luware Recording
THETALAKE
VERITAS
EY Shape the future with confidence
servicenow

Associate Sponsors

ACA
appian
droit
finregE
FIRST DERIVATIVE
globalRELAY
KAIZEN
kerv
MCO MyComplianceOffice
shield.
Thomas Murray
VERINT
VoxSmart
wordwatch
MOVIUS
INSIGHTFUL TECHNOLOGY

Exhibitors

GLOBAL
eflow
LEAP XPERT Responsible Business Communication
SCILA
SYMPHONY

XLoD Global London at a glance:

774 Attendees

7 Regulatory Speakers

38 Sponsors

116 Managing Director level speakers

94 Networking Sessions

47 Conference Sessions

Key takeaways

Balancing Priorities:

The current tough enforcement regime makes it harder for firms to align operational priorities with regulatory demands

Control Efficiency:

66% of attendees said that reducing the complexity and manual nature of the control environment was a top priority for 2025

Resilience Risks:

47% of attendees regard Cyber and Resilience as their top-priority emerging threats

Data Foundations:

75% of attendees regard core data quality and availability as the most significant data issue facing organisations, but both artificial intelligence (AI) and improved skills offer solutions

Regulatory Fragmentation:

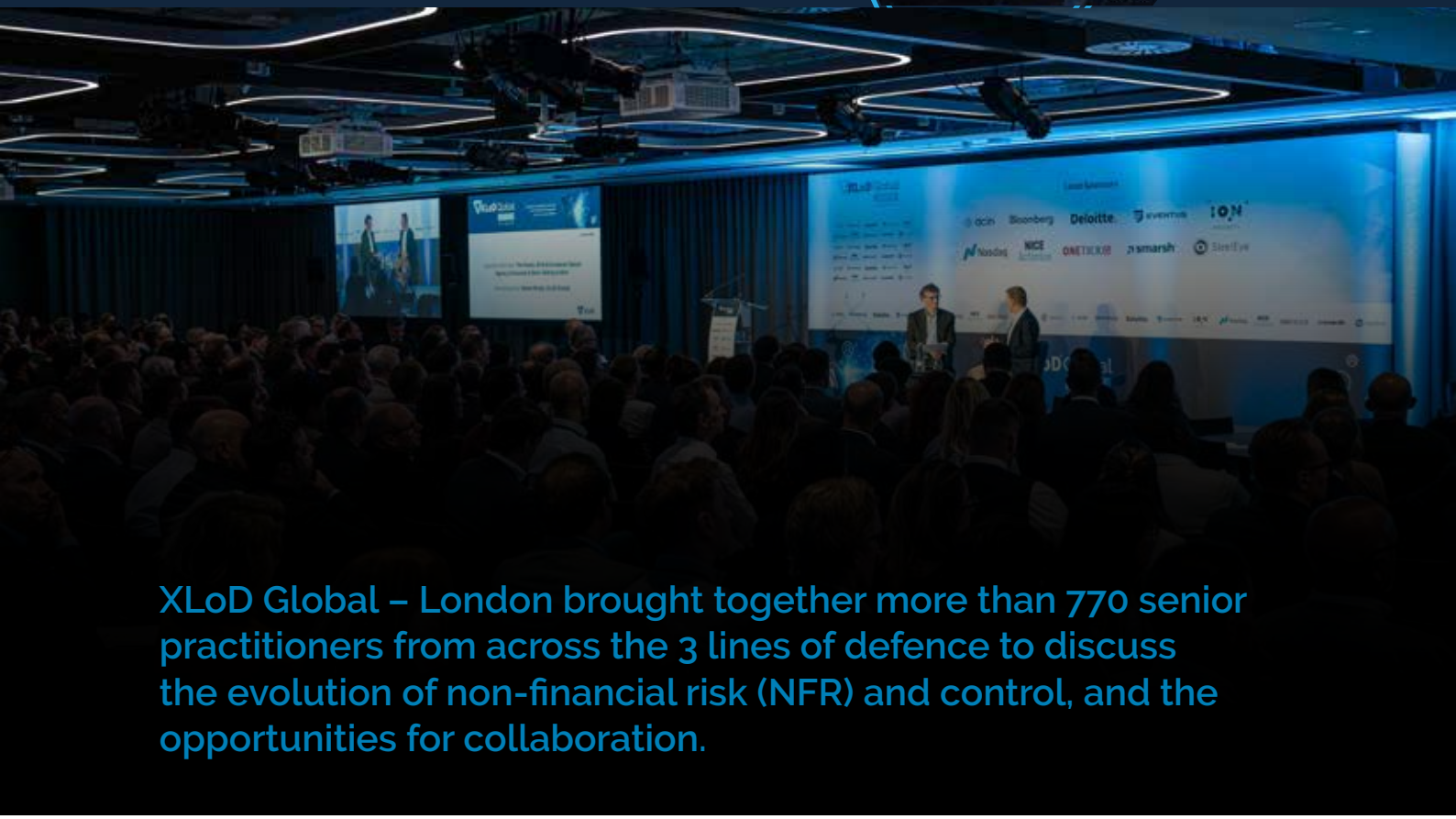
Compliance requires better collaboration and harmonisation to overcome inconsistencies across jurisdictions after Brexit

Risk Culture:

84% of attendees said that culture is more important than technical capability for supporting resilience and effective risk management

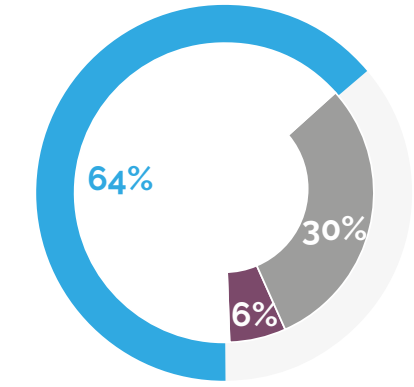
Technology Alignment:

Strategic, scalable adoption of technologies such as AI and voice surveillance can drive efficiency and competitive advantage



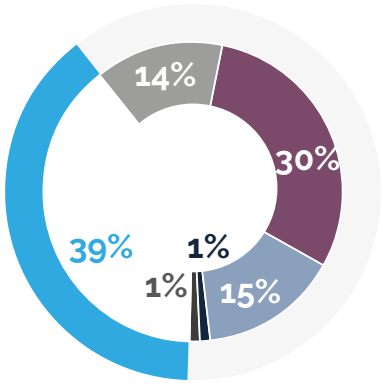
XLoD Global – London brought together more than 770 senior practitioners from across the 3 lines of defence to discuss the evolution of non-financial risk (NFR) and control, and the opportunities for collaboration.

Delegate profile by type



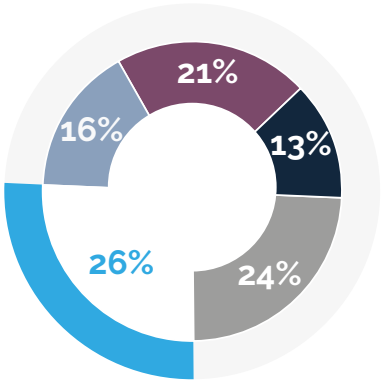
- Financial Institution
- Technology Vendor
- Consultancy

Financial institution delegate by corporate title



- Director
- Analyst
- Managing Director
- Manager
- Vice President
- N/A

Financial institution delegate by line of defence



- 2LOD - Compliance
- 1LOD
- 2LOD - Risk
- 3LOD - Audit
- 2LOD - Surveillance

"If you need to check in with peers and level-set on industry expectations and developments, this is the place to be."

JULIA HALE, COMPLIANCE OFFICER, BARCLAYS

Charting the Horizon of Risk & Control for 2025

XLoD Global explored the challenges and opportunities in managing NFR across the 3 lines of defence. Panellists acknowledged the increasing complexity of the risk environment and the difficulty of balancing regulatory priorities with internal challenges and commercial imperatives. They agreed it was essential to balance regulatory areas of focus and internal operational priorities, particularly in areas such as cyber, operational resilience, and data management.

They said that firms' priorities could become skewed because of the more aggressive enforcement environment, and that the dialogue between institutions and their regulators needs to be more nuanced. "One of the big challenges is ensuring regulatory prioritisation of, say, data doesn't override an institution's prioritisation of something like cyber, which may be more critical for day-to-day operations," one panellist said.

Data as the Foundation for Risk Management

Panellists agreed that improving data quality, visibility, and lineage was a persistent challenge given, as one attendee put it, data is "fundamental to everything we do". One reason for the current problems is the failure in the past to treat data as a strategic asset. "We're suffering from years of not treating data as an asset. To succeed in banking today, whether through personalisation or leveraging AI, you need good data," said one participant. The lack of ownership coupled with the fragmentation of data across systems pose a significant barrier to progress, but one way to overcome this problem is to use specialised data teams and improve the data literacy skills of employees. "Eight percent of my function are data specialists, and I ensure that the entire team undergoes data literacy training," said one of the speakers. "But it's not just about individual functions – it's about taking these skills into the wider organisation."

Attendees saw the potential for innovation through data: The application of advanced technologies, such as generative AI, can shift NFR functions towards predictive and proactive risk management. However, it would be a mistake to treat all data the same way. "Not all data is created equal. We need a thoughtful approach to what level of quality and lineage is required for different data attributes," one speaker said.

Resilience and Third-Party Dependencies

On the topic of operational resilience, panellists focused on the risks posed by third party providers and the associated cyber threats. Increasing reliance on just a few technology providers, such as cloud services, is a systemic issue. One panellist said, "I worry about third party dependency, not just from an institutional perspective but as a systemic issue. Regulators don't know how to control this, so they impose more requirements on what they can control – the regulated sector."

Resilience was also discussed in the context of regulatory expectations. Institutions strive to build robust frameworks while managing the associated costs. Streamlining controls and reducing their manual nature are priorities. "We've built effective control environments, but they're incredibly labour-intensive and expensive. Much of that is because we've created

silos for different risks – cyber, fraud, conduct – when 90% of the controls are the same," one participant said.

Adapting to Emerging Risks

Emerging risks include technological advances and regulatory changes, as well as the adoption of new technologies such as AI, which can be both a risk and an opportunity. "We must embrace technology like AI. It's here, and it's becoming part of our day-to-day," one speaker said. However, they also highlighted the need for robust controls, particularly when using generative AI (GenAI) for tasks such as compliance alert triage.

Then there are conduct risks associated with the use of unauthorised communication platforms, such as WhatsApp: Some participants suggested a blanket ban was the best approach, while others recommended controlled adoption supported by technology. "We cannot keep forcing employees to use outdated tools while banning the platforms they find convenient. It drives behaviour underground," one participant said.

The broader regulatory environment may also be a source of uncertainty, particularly if geopolitics leads to divergent approaches. "With the changing political landscape in the US and other regions, we may see regulatory chaos – one side pushing back while the other doubles down," one speaker warned.

Optimising Resources and Skills

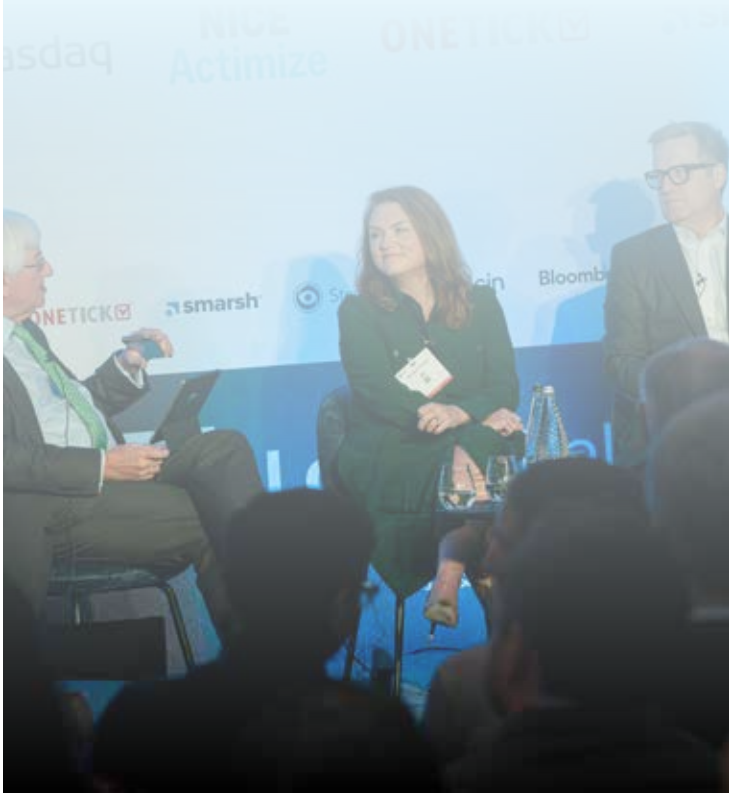
Panellists broadly agreed that organisations have sufficient resources to tackle the main problems, but criticised how those resources are deployed. "It's not about quantity; it's about whether we're using resources effectively and whether we have the right skills," one panellist said. Firms need to put more emphasis on skills in areas such as data analytics and systems thinking.

Another important issue is ensuring that the 1st, 2nd, and 3rd line functions are aligned, as this is key to improving the overall efficiency of NFR management frameworks. "The gap between 1st and 3rd lines is closing, but it's the 1st line moving closer to where the 3rd line is – not the other way around," one participant said.

Panellists stressed that functions should not forget the importance of innovation, efficiency, and collaboration in addressing problems and inefficiencies.

The Regulator's Viewpoint: Balancing Innovation, Regulation, and Market Stability

Regulators discussed the top themes facing the industry including: balancing stability with innovation; regulatory fragmentation; evolving risks from emerging technologies; and tensions between data privacy and regulatory oversight. In a poll, **68% of attendees** said that overall, the input from regulators has been helpful. However, there is room for improvement with regulators hindering banks' innovation.



Balancing Stability with Innovation

At XLoD, regulators discussed how they can best support market stability while fostering financial innovation. The increasing focus on AI and machine learning (ML) was described as a double-edged sword because it offers unprecedented opportunities for efficiency but introduces novel risks. "We have to understand how algorithms interact with each other," one regulator said, highlighting concerns about market manipulation when self-learning algorithms make independent trading decisions. There needs to be greater collaboration between regulators, banks and academic institutions to understand the underlying technology and its implications.

Firms have a responsibility to understand and control their algorithms, even when these systems become more complex and autonomous. Regulators stressed the importance of accountability, urging firms to ensure that they can explain and justify the decisions made by their AI-driven systems.

Regulatory Fragmentation and Cross-Jurisdictional Challenges

The European regulatory framework allowed for a degree of harmonisation, but after Brexit, when the UK left the EU, it became harder to cooperate and share data. "It's no longer possible to have automated information exchange with the UK," one regulator said. Formal requests to exchange data take extra time and resources. Despite these hurdles, participants praised the strong case-by-case cooperation between EU and UK regulators, particularly in areas such as criminal market misconduct.

The problems of regulatory fragmentation were also explored through the lens of operational resilience. Firms operating globally face different requirements in the US, UK, and EU, which complicates their compliance efforts. Regulators noted their commitment to improving cooperation and reducing duplication by using international initiatives such as IOSCO.

Firms' Frustrations and the Need for Clarity

One of the main frustrations for firms is a lack of clarity in regulatory expectations: In a poll conducted during the session, 38% of attendees complained about this (which was at least an improvement from the previous year's 50%). One regulatory speaker described the inherent tension: "Nobody wants a tick-box regulator, but every firm would love a list to tick off." Regulators said that prescriptive rules might provide clarity but could stifle innovation and constrain businesses, adding that firms often try to comply with the bare minimum. This is an issue when regulations are designed to encourage proactive compliance. Regulators said firms need to define key terms such as materiality themselves and show that their compliance frameworks are adequate.

Emerging Risks from AI and Market Volatility

AI adoption presents unique governance challenges, including the validation of models and the ability to explain their outputs. "Firms need to demonstrate to us that the model is working. Don't claim that your vendors don't give you transparency to the models, because that's the firm's responsibility to demonstrate compliance, not the vendor's," one regulator said.

Market volatility is another area of concern, driven in part by the increasing use of automated trading in fragmented and less liquid markets. The concentration of passive trading towards the end of the day was identified as a structural risk, with implications for market stability. Regulators monitor these trends closely to assess their impact on liquidity and volatility throughout the trading day.

Data Privacy vs Regulatory Oversight

The tension between data privacy and regulatory oversight was a recurring theme: Regulators acknowledged firms' concerns over complying with local data protection laws while meeting international regulatory requirements. However, firms were told they should not use privacy laws as a way of avoiding transparency. "We respect privacy, but we can't have firms hiding behind it to avoid scrutiny," one regulator said. Proportionality was presented as the guiding principle, with regulators focusing their data requests on specific cases where there was a clear need for oversight.

Panellists agreed that cooperation among regulators, both within and across jurisdictions, was critical to addressing the complexities of modern financial markets. Emerging technologies such as AI, the growth of passive investments, and the evolving structure of liquidity require attention: regulators and firms must navigate these challenges together.

"Fantastic networking event with industry leaders and risk & control professionals packed with insights and foresights which shape our roles and industries."

AARON ROTHERHAM, AUDIT DIRECTOR, CITIGROUP

"Valuable conference with many connections made and opportunity to re-connect in person with ex-colleagues."

ALISON SMITH, CHIEF AUDITOR, UK, CITIGROUP

CASE STUDY:

A View from the Board: Evolving Non-Financial Risk Management in Financial Services

1LoD brought together senior board practitioners to discuss NFR management frameworks in 2024 and the critical need for evolution in the face of rapid technological advances and interconnected risks.

Data and technology are essential to driving transformation. Board-level executives expect a significant shift in the next 5 to 10 years, underpinned by advances in AI, automation, and analytics. They see data as the cornerstone of modern risk management, describing it as "the new oil." However, they said that its effective use required robust data-management practices, including security, quality assurance, and flexible frameworks capable of accommodating changing demands.

Participants discussed the interconnectivity of risks and the implications for operational resilience. They noted the increasing complexity of threats stemming from global interdependencies, third-party relationships, and geopolitics. One panellist said that risks are no longer limited to individual institutions but often extend across supply chains and industries, making scenario-planning and collaborative approaches essential. "The interconnectedness of markets creates vulnerabilities that require proactive management and detailed contingency plans," one participant said. And while regulators have introduced resilience tools, such as impact tolerance frameworks, these are relatively immature, so organisations must do more to refine their approach.

Regarding Environmental, Social, and Governance (ESG) risks, participants said that there has been progress in addressing climate risks, with significant focus on disclosures and sustainability frameworks, but that the social and governance dimensions often play second fiddle. Many organisations integrate ESG as a transversal risk across existing taxonomies, aligning it with product suitability, counterparty due diligence, and reputational risk processes.

Group heads acknowledged regulatory and organisational challenges in implementing these changes. They cited significant obstacles – such as jurisdictional barriers to sharing data and localisation rules – particularly for global institutions. While technology is an enabler, the need for high-quality data and the reluctance of organisations to invest heavily in foundational improvements were recurring problems. One speaker said, "Without addressing these underlying issues, progress will remain piecemeal."

Enhancing the Effectiveness of the 1st Line

Over the two days of XLoD, senior 1st line risk and control practitioners discussed the challenges, associated opportunities, and the evolving practices in managing NFR within the 1st line. Participants considered the maturity of the 1st line model, the need for collaboration across the 3 lines of defence, the role of technology in enhancing efficiency, and the implications of increasing regulatory scrutiny.

The Maturation of the 1st Line Model

The 1st line has evolved into a credible and structured function, integral to managing NFR. One participant said that it now serves as a "structured professional team within the non-financial risk space," fostering a common language between business units, 2nd line functions, and auditors. However, it is important that the 1st line supports and influences without stepping over the line into accountability, which remains with business heads. "It's a tricky balance," one speaker said. "The 1st line must help and direct without taking over or being seen as accountable for aspects of supervision." Participants said it was important not to overburden businesses with operational tasks and time-wasting busy work, but to focus on strategic objectives and risk mitigation.

Collaboration Across Lines of Defence

A recurring theme was the need for better collaboration between the 1st and 2nd lines to reduce duplication and improve efficiency. One panellist described this as an ecosystem approach: optimising the 1st line would only work if there were coordinated efforts across all lines of defence.

One participant described how their organisation recently consolidated compliance assurance and 1st line testing teams into a single testing centre of excellence led by the 1st line. "We've created a global testing function that eliminates duplication," they said. This improves efficiencies as different teams no longer test the same processes multiple times, while still retaining independent review and challenge.

Standardisation and Technology

The fragmented and complex nature of control environments is a pressing issue. Many institutions have accumulated disparate controls over time, often in response to regulatory or audit findings, leading to inefficiencies and inconsistency. "Banks grew up slapping on additional controls in response to individual issues, creating an environment that is now bloated, fragmented, and manual," one speaker said.

These inefficiencies can be addressed using standardisation and automation. Leveraging technology, including RegTech solutions, can streamline processes, save costs, and improve regulatory compliance. One speaker described the value of automating and

rationalising control inventories: "Using AI tools, we've rewritten 10,000 controls in a fraction of the time it would have taken manually, saving 90% of the associated costs."

Regulatory Pressures and Strategic Responses

Regulatory requirements have a significant influence on 1st line practices. Many panellists said that institutions often focused on meeting immediate regulatory demands rather than adopting long-term strategic solutions. "Regulators don't expect everything to be fixed overnight, but they do expect firms to show they're on the journey," one participant said. They want to see a shift from reactive detective controls to proactive preventive controls, but this can lead to other complications. "Preventive controls can be effective," one speaker said, "but they come with costs. If implemented poorly, they can introduce other risks or slow down processes, particularly in trading environments."

Despite the updated UK Corporate Governance Code requiring a board of directors to oversee the effectiveness of key controls, 64% of attendees said that their respective boards had insufficient understanding to do so.

Building a Strong Risk Culture

A robust risk culture underpins successful risk and control functions. "You can implement the best systems and processes," one panellist said, "but without a strong risk culture, none of it works." This cultural alignment, starting with the leadership and permeating all levels of an organisation, is critical. One participant described their experience of getting the leadership to adopt a more agile and modular risk framework: "Simplicity is key. It's easy to make things complicated, but the real challenge lies in simplifying and focusing on what adds value."

Industry Collaboration and Mutual Benefit

Greater industry collaboration is required to address common challenges, particularly around standardisation and regulatory engagement. "There's no competitive advantage in one bank getting things right while another struggles. If one institution ends up on the front page, it reflects poorly on all of us," one participant said.

As another participant put it: "It's about stepping back, simplifying, and leveraging what we have – both internally and across the industry—to build something that works now and evolves with us."

The need for standardisation, collaboration, and technology adoption was a unifying theme, while regulatory demands continue to shape priorities. The panellists agreed that achieving balance – between preventive and detective controls, between operational efficiency and regulatory compliance, and between innovation and optimising legacy practices – was key to the future success of the 1st line.

CASE STUDY:

Navigating the Interconnected Landscape of Emerging Risks

A theme emerged throughout the conference on identifying and managing emerging risks in an era marked by interconnected challenges, including heightened cyber risks, geopolitical tensions, technological advancements, and climate change. Attendees highlighted how these risks are not only escalating individually, but are also increasingly interconnected, creating greater complexity in their management. One participant observed that "it is not just that each of the emerging risks have an unprecedentedly high degree of volatility, but the connectivity of these risks and that is the that's the challenge of the day," illustrating the difficulty of addressing these overlapping vulnerabilities.

Cyber resilience emerged as the most prominent concern for the audience and panellists alike. With the increasing frequency of cyber-attacks, the dependence on third-party vendors and critical systems was identified as a key vulnerability, with one panellist noting that "organisations often fail to understand their end-to-end processes, and this creates significant exposure during cyber events." 1st line practitioners were called upon to move beyond a reliance on contractual assurances and play an active role in understanding and managing the cyber capabilities of third parties. This sentiment was echoed in discussions about enhancing collaboration both within organisations and across the industry to address shared challenges such as vendor risks and system interdependencies.

Regulatory risks were described as both a longstanding and evolving concern. While compliance has always been a core focus for financial institutions, the panellists stressed that implementation challenges now pose an equally significant threat. One speaker explained that "the cost of non-compliance far outweighs the cost of compliance," highlighting the need to integrate regulatory requirements into broader business strategies. Another attendee reflected that "regulatory expectations should be viewed as an opportunity to enhance systems and controls rather than a burden." They noted that regulatory imperatives, which often lead to additional resourcing, can be used to change not just what the regulator's want, but also systems that require further investment.

The conversation also turned to the human dimension of managing emerging risks. Panellists noted the difficulties of bridging generational gaps within organisations, particularly as younger employees bring different perspectives and expectations to the workplace. One participant remarked that people risk is now heightened, and it is the responsibility of senior management to "empathise with new generations entering the workforce to retain talent and ensure a cohesive approach to risk management."

"All of the speakers were very credible and insightful. They answered relevant questions with specifics."

JAMIE CROCKER, HEAD OF NFR PORTFOLIO OVERSIGHT, CB, IB & CB IB OPERATIONS AND CONTROLS, DEUTSCHE BANK

"1LoD provided me with an opportunity to learn from and share knowledge with industry experts during the roundtable and panel sessions."

MACIVAN DAVIES, VICE PRESIDENT, IT AUDIT, MIZUHO

Climate risk was another area of focus, with one panellist asserting that "climate risk is going to be the thing of our era. It's not a question of whether or not it's an emerging risk. The question is, when does it become material and overwhelming? Climate, climate risk and the manifestations of climate risk are already here." While some in the audience ranked it lower on their list of priorities, the panellists argued that its impacts—ranging from operational disruptions caused by physical risks to financial implications from credit rating downgrades—are already present.

"Climate risk is going to be the thing of our era. It's not a question of whether or not it's an emerging risk. The question is, when does it become material and overwhelming?"

The lack of threat-specific knowledge and resources was identified by the audience as another major challenge in managing emerging risks. Panellists emphasised the need for "master generalists" who can bridge silos within organisations, convene the right experts, and translate complex risks into actionable insights for business leaders. This ability to connect the dots across different risk domains was described as critical for navigating the increasingly complex risk landscape. As one participant summarised, "adaptability and collaboration are key to navigating the unknowns of emerging risks."

Navigating the Road to Operational Resilience: Challenges, Progress, and Strategic Opportunities

As firms prepare for upcoming regulatory deadlines in 2025 and consider the commercial benefits of maintaining resilient business services, operational resilience is attracting more attention. XLoD attendees discussed industry progress, the significance of third party management, advances in scenario testing, embedding resilience into governance structures, and the strategic potential of resilience initiatives.

Progress Towards Regulatory Preparedness

Most organisations are already preparing for operational resilience regulations. A poll showed that 72% of firms consider themselves mostly prepared, whereas 26% said they still need to do significant work. One participant noted, "We are at the start, not the end of this journey." Highlighting that as regulations evolve and the industry provides feedback, further progress can be expected.

The Digital Operational Resilience Act (DORA) is particularly challenging because of its prescriptive nature. Participants said that specific requirements, such as those concerning critical third-party dependencies, are complex, requiring further clarification and adaptation over time. Organisations have collaborated through trade bodies and sector groups, making it easier to share knowledge and align with others across the industry.

Third-Party and Critical Dependencies

Managing third-party risks is a central challenge, according to a poll. "Many third parties are also our clients," said one attendee: This shows the interconnected nature of the industry and banks, which must provide assurances about their own resilience to other market participants where they have critical dependencies. Panellists stressed the need for enhanced third party assessments, stronger vendor management processes, and better engagement with regulators to ensure compliance. One participant remarked, "When you look at DORA, when you look at the technical standards associated to it, there's a lot that we really need to work through practically. It is about establishing that foundational position and recognising that's going to iterate over time. I think there's a lot of questions that have to be had between clients and third parties to make sure that we're all compliant."

The discussion about critical third parties, including cloud service providers, showed the need for both interoperability and substitution in case of vendor failure. "The cloud providers are probably far more resilient than most organisations because they've got zones and regions in terms of building resilience," one speaker said: "Nonetheless, the regulators will start to ask the question what happens if they are just not available to you." Panellists agreed that portability of data and services between providers is still a challenge, exacerbated by the cost and lack of

standardised structures. While cloud providers are often highly resilient, firms still need to prepare for scenarios where services might be unavailable.

Advances in Testing and Scenario Planning

Testing and scenario planning are essential to operational resilience. Participants stressed that traditional tabletop exercises, while valuable, are insufficient to capture the complexities of live incidents. Increasingly, firms adopt live technical testing and incorporate stress-testing specific scenarios. "We must hammer the weak spots to see if they exist, then remediate, rinse, lather, and repeat," one participant noted.

One panellist described the 2025 deadlines as "the starting point rather than the finish line," and stressed the need for continuous assessment. Firms must challenge assumptions and move beyond 'happy path' scenarios to test worst-case outcomes. The CrowdStrike incident in July 2024 showed that organisations need to ask different questions about vendor risks, such as how infrastructure might behave if a service 'took itself down'.

Embedding Resilience into Organisational Culture and Governance

Embedding resilience into organisational structures and culture is crucial. Panellists noted the importance of adapting operating models to ensure enterprise-wide oversight of resilience risks, and said resilience should be for everybody, requiring strong collaboration across the 1st and 2nd lines of defence. This included ensuring that business, risk, technology and other key functions were appropriately involved in resilience initiatives.

Participants discussed the role of governance, stressing the importance of integrating resilience into decision-making processes and risk-appetite frameworks. Embedding resilience in the organisation "is not a one and done exercise, it should be ongoing. It's a very big issue from the regulators" noted one attendee and requires continuous monitoring and reporting. Effective communication is a key tool in managing crises and maintaining resilience.

Resilience as a Strategic Opportunity

Beyond meeting regulatory requirements, resilience can enhance organisational adaptability and customer trust: It could even be used as a differentiator, allowing firms to demonstrate their robustness to clients and stakeholders.

Panellists discussed the benefits of industry collaboration, particularly in developing standardised approaches to third-party assurance and testing. While acknowledging the challenges, one participant said, "there is an opportunity for cultural change, as we work with third parties to align on resilience objectives."

Operational resilience is both a regulatory requirement and a strategic opportunity, but also brings certain problems, particularly in managing third-party dependencies and advancing testing sophistication. Panellists said there must be continued collaboration, innovation, and a focus on embedding resilience into organisational culture to navigate the regulatory changes successfully.

The Evolution and Challenges of Modern Surveillance:
Trade, Communication, and Voice in Focus

Evolving Challenges and Innovations in Trade Surveillance

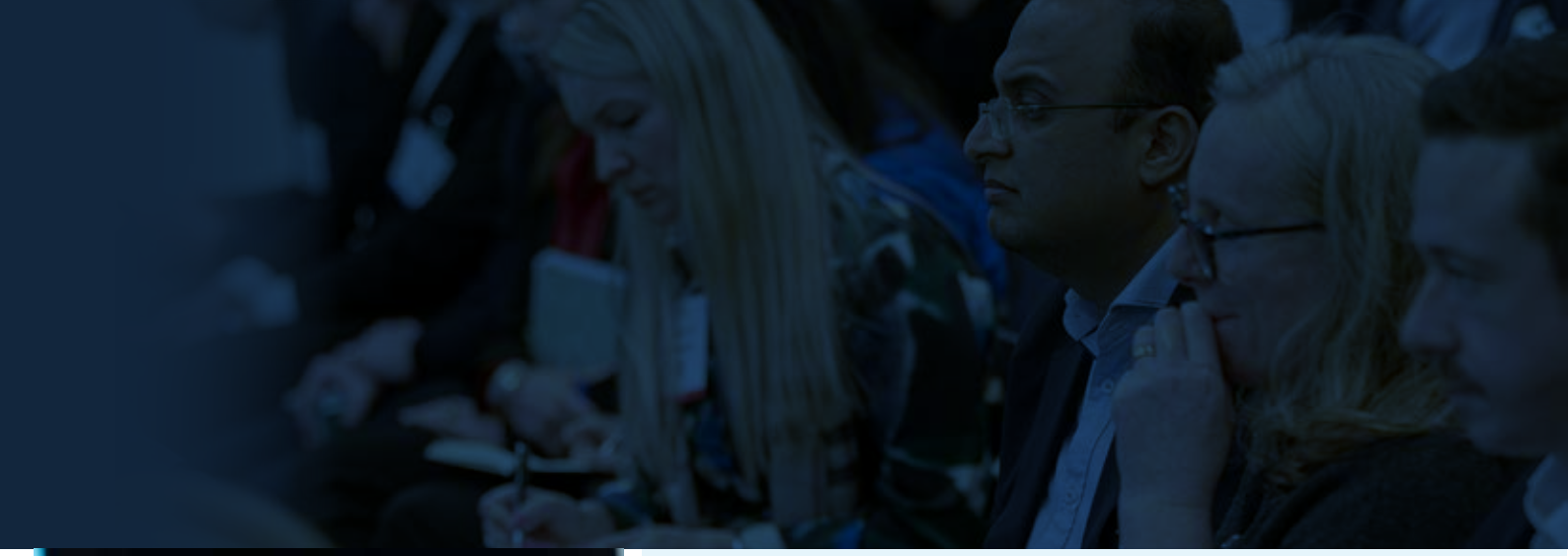
Surveillance leaders described how sophisticated trading strategies have led to surging trade volumes, necessitating advances in surveillance technology to manage capacity, refine detection parameters, and address cross-market risks. One speaker noted the importance of tailoring surveillance approaches, stating that a "one-size-fits-all strategy may not be ideal" given the varying nature of client activity and trading patterns.

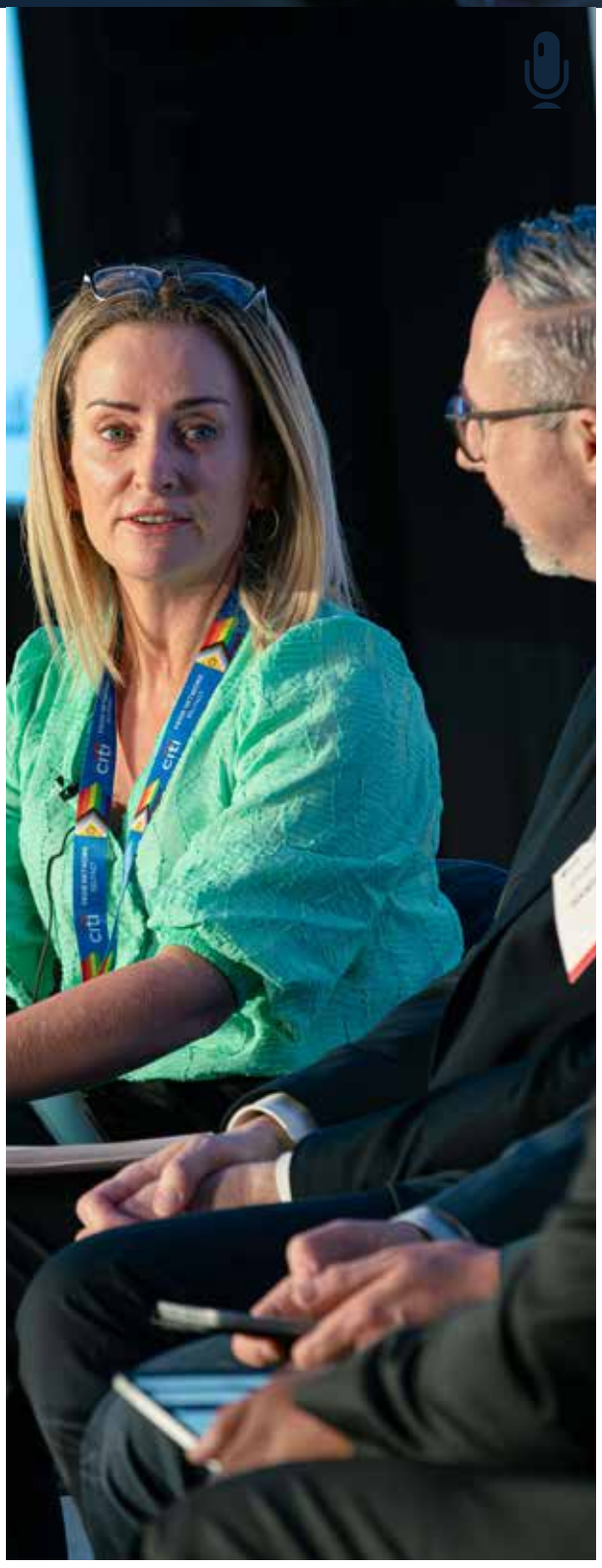
Firms have finite budgets, and this can lead to tensions between competing departments. Many institutions have shifted their focus from increasing headcount to investing in advanced tools. One participant described how modular systems allowed for "real-time tuning and optimisation". While enforcement actions are a critical driver for funding, panellists said reputational risk and operational efficiency are increasing in importance.

Participants said the adoption of AI and ML in trade surveillance is slower than in communication monitoring. AI applications, such as clustering techniques and automated deep dives into data, were identified as valuable for detecting anomalies and enhancing alert prioritisation. One panellist said that although AI's impact in trade surveillance was less visible than in communication tools, "there is exciting innovation happening in the space."

With the increasing regulatory focus on governance and data integrity, speakers stressed the importance of continuous improvement. One said that regulators welcomed strategies such as "below-the-line tuning" to ensure thresholds were effective without compromising detection. Regulators now ask more granular questions about data completeness, so firms need to be sure they can explain and defend their surveillance programmes. However, many practitioners complained that regulators are expecting deep dives into data quality, but not allowing enough time for meaningful feedback, leaving banks to interpret expectations.

Given the recent regulatory fines and proliferation of trading venues, participants agreed that non-compliance is expensive, and that self-disclosure does not necessarily mean exemption from large fines. One speaker said, "funding and resourcing are challenging to get in order to do the things that you need to do, and the short-sighted view of 'we do not want to spend this money up front now' will not fly – firms need to realise it is in fact cheaper to fix some things now, than face regulatory consequences and enforcements."





The Evolving Landscape of E-Comms Surveillance

In discussing communication surveillance, panellists said that regulators – particularly in the US – have tended to target and fine those firms which failed to capture business-related communications, often conducted over unauthorised channels such as WhatsApp.

The panel explored how firms are adapting their compliance frameworks to meet these changing demands. One speaker said that regulators "expect a firm-wide policy on the use of electronic communications, supported by training, attestations, and evidence of disciplinary measures". Another warned of the growing expectation for firms to demonstrate channel completeness, linking it to the risk of undermining regimes such as the prevention of market abuse. Panellists also discussed the increasing focus on non-financial misconduct, such as bullying and discrimination, and the Financial Conduct Authority's (FCA) expectation for firms to have systems in place to identify such behaviours.

One participant, discussing technological changes, noted that "generative AI and advanced technologies now enable a level of data completeness and risk detection that was previously impossible," suggesting that regulators will likely raise their expectations in response.

In future, the FCA is expected to conduct surveys to benchmark firms' preventative controls. One panellist concluded that to succeed, firms need to "enhance governance, ensure data completeness, and adapt frameworks to emerging technologies and risks." The consensus was that regulatory scrutiny would only increase, requiring firms to adopt more sophisticated tools.

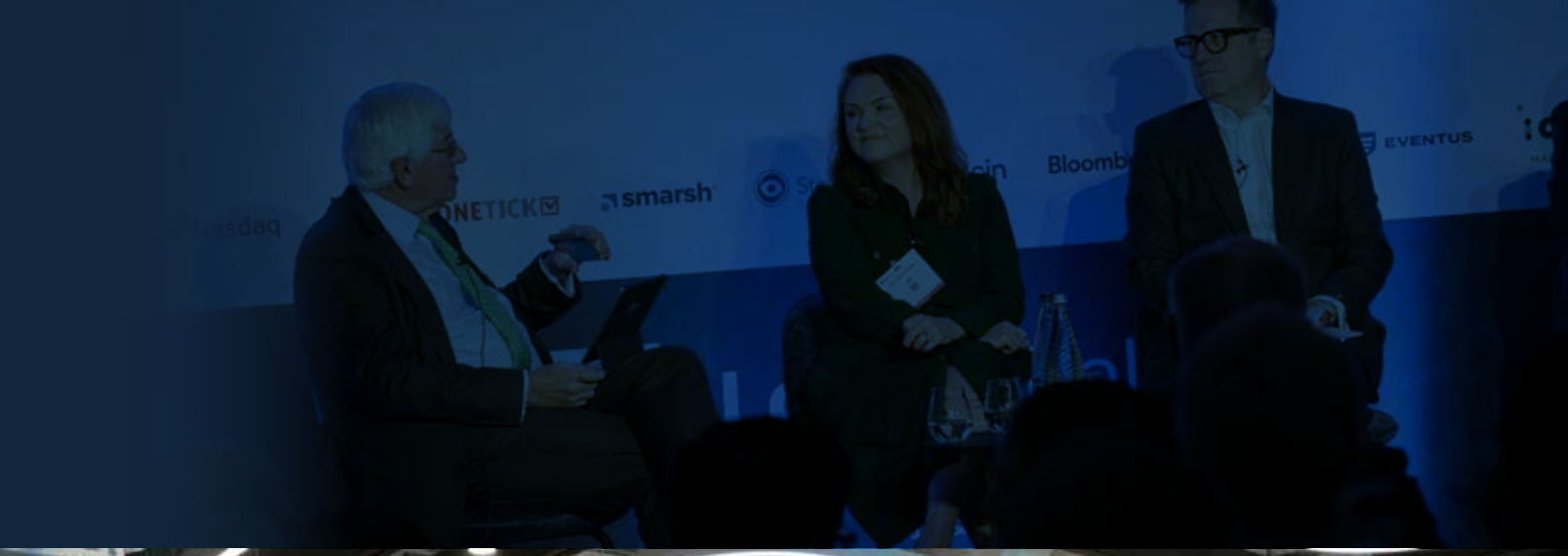
Shaping the Future of Voice Surveillance

A discussion of voice surveillance, one of the most complex areas of surveillance, focused on technological advancements, regulatory pressures, and business use cases. Participants agreed that transcription technology has improved significantly, with "near-perfect accuracy" now achievable even for complex, multi-language scenarios. However, there was much debate about whether firms were ready to use these tools. One panellist said, "The technology is better than the human ear, but confidence in it is still building."

Regulatory expectations are a key driver for broader adoption, and the FCA's focus on non-financial misconduct, such as bullying and harassment, has expanded the scope of surveillance. "We are seeing conduct risk flagged more frequently than market abuse in voice monitoring," one participant observed. Another added, "The regulator may soon demand more comprehensive coverage as technology evolves."

The potential for voice surveillance to deliver front-office benefits was also discussed. Real-time transcription can reduce operational errors and enhance decision-making, although it was acknowledged that "real-time surveillance for market abuse detection lacks a clear business case." While sentiment analysis and tone detection were seen as valuable future capabilities, attendees said that this was secondary to achieving foundational accuracy and data quality. Real-time monitoring was similarly identified as more applicable to front-office efficiency rather than surveillance needs, with limited regulatory business cases at present.

> ***While sentiment analysis and tone detection were seen as valuable future capabilities, attendees said that this was secondary to achieving foundational accuracy and data quality.***



"XLoD Global - London is the only event that brings the senior compliance executives and all the vendors to a single location for the most compelling surveillance event of the year."

PAUL TAYLOR, VICE PRESIDENT PRODUCT MANAGEMENT, SMARSH

"The subject matter was spot on, the coverage of different areas of surveillance and roundtables were really good. the large attendance of my peers in the market made this extremely relevant."

GRAHAM ROOKE, SURVEILLANCE, SMBC

CASE STUDY:

The Evolving Role of Legal and Compliance in Regulatory Compliance

A central theme at XLoD Global was the interaction of legal and compliance functions within organisations, especially in the context of regulatory frameworks. Discussions highlighted varying approaches to positioning legal within the 3 lines of defence model, with some firms removing legal from the model entirely to clarify its multifaceted role.

Legal's Placement in the 3 Lines Model

Organisations have different views about where legal fits within the 3 lines of defence framework. While some firms placed legal in the 1st or 2nd line, others put it outside the model to mitigate role ambiguity. One participant explained their organisation's rationale: "We're going to have to take legal out of the 3 lines of defence because it's a different set of activities and it makes it much cleaner, with a lot less debate, because our lawyers felt their role had been inadvertently compromised by putting them in the 1st line. In our next refresh, they're going to move out of the 3 lines of defence." This shows the importance of preserving legal's independence and advisory role, ensuring it remains distinct from operational responsibilities.

Overlapping Roles and Cultural Nuances

Participants acknowledged that legal's responsibilities often overlap with compliance, complicating the delineation of roles. One participant said, "legal operates in both the 1st line and 2nd line depending on the activity, and it's not always straightforward to differentiate these roles." For example, legal's involvement in executing contracts aligns with 1st line operations, whereas advising on litigation strategy fits a 2nd line advisory capacity.

The dynamic between legal and compliance also varies depending on an organisation's structure and culture. Attendees emphasised the importance of collaboration, particularly in addressing complex regulatory requirements. One panellist said, "You need your lawyers to be thinking about potential litigation strategy. I just don't think you can write it down in a way that creates this really simple 'You stay in that lane, we stay in this lane'. It's the partnership that we really invest in." However, participants stressed that effective collaboration must not undermine accountability in the 1st line, which remains responsible for managing risks and decision-making.

Principles-Based Regulation and Supervisory Expectations

A significant challenge is how to interpret principles-based or outcome-focused regulations, which lack the precision of rules-based systems. The UK's Consumer Duty is a prime example, requiring firms to consider a "range of reasonable responses" to meet regulatory expectations. This often necessitates collaboration between legal and compliance to provide comprehensive advice. Another layer of

complexity arises from supervisory expectations which, while not codified laws, exert considerable influence. As one panellist put it, "you've got to either comply with these expectations or have a serious appetite for taking on your regulator."

Conservatism in Legal Functions

The discussion about whether legal functions are too conservative showed a near-even split among attendees – 48% agreed, 44% disagreed. Some argued that legal should be viewed as an enabler rather than a blocker. One participant said, "You do need to start looking at your 1st line and how mature they are, because there may be reasons people have to say no: is the proposition sensible and isn't going to guarantee sustainable P&L returns for the business?" In other words, perhaps firms need to address the shortcomings of the 1st line rather than blaming the legal department.

Balancing Legacy Systems, Innovation, and Compliance in NFR Technology

Participants discussed the use of technology in managing NFR, including the complexities of maintaining legacy systems, the pressures of compliance, the strategic alignment of technology decisions, and the integration of emerging tools like AI.

Legacy systems play a role in financial institutions and, despite significant advances in technology, many banks still rely on mainframes and outdated archives because of their reliability. However, the costs of maintaining such systems, coupled with their limitations in adaptability, are a problem. "Everybody still has mainframes for very specific use cases. Who would have thought, 20 years ago, when cloud computing emerged, that mainframes would still be chugging away?" one participant said. Replacing these systems costs time and money. Even when new technologies are introduced, older systems are rarely retired, leading to bloated infrastructures that are expensive to maintain, and require additional and often different data requirements to newer systems.

A discussion about enterprise technology strategies found that in many cases, these are not aligned with the needs of compliance and non-financial risk management: 81% of attendees polled during the session said enterprise technology decisions were taken without sufficient regard for these functions. More broadly, even though risk and compliance are regarded as important, they are often treated as an afterthought rather than a strategic partner. However, some organisations have successfully integrated compliance into their broader technology strategies, by fostering strong partnerships between compliance teams and other business units and ensuring they have a seat at the table when key decisions are made. "When compliance has a seat at the strategic table, the conversations are more aligned, and the outcomes are far more impactful," one participant said.

Another point of friction concerned data silos. Banks tend to have fragmented data systems which hinder operational efficiency and compliance efforts, while maintaining multiple systems which replicate similar functions wastes money. One participant said a major institution had conducted an internal survey and found it had 134 different security masters, thus duplicating its resources on a massive scale. Although some organisations try to consolidate data into unified frameworks, this approach is fraught with challenges, including the high costs of systemic change and the risk of adopting technologies that may become obsolete. Instead, many institutions opt for tactical solutions, addressing individual data problems without committing to overarching transformations, which adds to the issue of multiple disconnected systems.

Banks are exploring AI to enhance content generation, developer productivity, and customer assistance, but need to be careful. "Have you figured out where and how you're going to be doing your AI implementation? Do you have the expertise, the staff? Has anybody calculated the compute resources being able to be dedicated to this, the training datasets, all the annotation guides? You need to go through that

> ***One participant said a major institution had conducted an internal survey and found it had 134 different security masters, thus duplicating its resources on a massive scale.***

education process because even now, as people are looking at new technologies and innovation, there's always an irrational exuberance. Everybody just wants to do it for the sake of doing it," one speaker said. The compute and storage costs associated with AI models, as well as the complexity of managing and securing data, are substantial. Organisations are starting to establish governance frameworks to control these costs and prioritise the most impactful use cases. For instance, one firm outlined its focus on scalable applications of AI rather than pursuing numerous fragmented projects. "We agreed to focus on large-scale themes, like policy assistance and summarisation, rather than running 100 different experiments," one participant said.

The panel also addressed the broader concept of total cost of ownership (TCO) in technology. While the idea is widely recognised, its application is inconsistent. Many organisations struggle to calculate the TCO of their technology stacks, leading to inefficiencies and missed opportunities for cost savings. One participant said, "It's easier to buy new technologies and add them to the stack than to remove old ones," which contributes to escalating costs and complexity. The discussion concluded that better governance and decision-making frameworks are needed to ensure that technology investments are aligned with business goals and compliance requirements.

Some organisations have successfully fostered collaboration across departments and implemented strategic initiatives. Agile working methodologies are an example of how technology teams can deliver more value by working closely with business stakeholders. One participant said, "If we're going through an agile transformation, it's not just that it needs to transform, it's the business needs which may require a different mindset as well. We've seen the need for the business to buy into being the product owner and actually prioritising the backlog and saying what's important to them as that can be beneficial as well, not just pure technology."

Banks recognise the value of simplicity, from consolidating data systems to streamlining controls. One participant described their firm's efforts at rationalisation – turning 500 controls into 20 key controls, and consolidating multiple supervision systems into a single platform. Such initiatives reduce costs and make systems easier to manage and adapt.

Financial institutions can transform their technology and build more resilient, efficient systems, provided they focus on simplification and on scalable initiatives which have an impact. "Reusing what's there is way better than building from scratch, but it takes a mindset shift across the organisation to make it happen," one participant said.

The Evolving Role of Internal Audit: Strategic Alignment, Innovation, and Resilience

The role of internal audit within financial services has evolved from an observational, outputs-focused function to one that is strategically aligned, outcomes-driven, and deeply embedded in organisational governance. As a result, internal audit has remained relevant despite significant changes in the industry – such as advances in technology, and greater regulatory and stakeholder demands.

Auditors are now expected to attend executive committees and risk-management meetings, where their input must align with strategic organisational goals. As one internal auditor put it, "We absolutely have to be present, have a voice, and provide challenge in an independent way." Examples of innovative practices, such as real-time audits and enhanced continuous monitoring, were shared during the sessions, showing how audit teams adapt to provide timely assurance on live risks.

Building trust is a cornerstone of effective auditing. The panellists agreed that to win trust from stakeholders, audit must demonstrate credibility, knowledge, and the ability to escalate issues appropriately. Trust is built through consistent engagement, not only during difficult times, but also when recognising positive outcomes. An auditor's ability to understand and agree with the business's objectives is fundamental to creating this trust. As one speaker said, "It's about showing we understand what they're trying to achieve and focusing on the long-term sustainability of the organisation."

An exciting new development concerns the integration of AI and ML within internal audit functions. While many organisations were still in the early stages of adoption, the panel noted the potential for AI to transform auditing by automating repetitive tasks, improving sample selection, and enabling faster analysis of both structured and unstructured data. Internal auditors could leverage tools such as GenAI to draft testing strategies and identify trends, although this practice is not yet widespread. One panellist urged organisations to "start doing it right now," adding, "I would start looking at the ways that you can engage in line with your own organisation's policy with some of these external tools that exist, and you can do it without loading up any of your own data – that is the most effective way of using generative AI." While advocating the use of external AI tools as a means of gaining efficiencies while adhering to organisational policies, speakers acknowledged that to get the most out of it, firms need to have practitioners with the right skillsets so that they can effectively use the tools and derive real insights from these tools.

Panellists also discussed how internal audit functions were conducting real-time audits and deep-dive reviews to assess organisations' preparedness for operational resilience, particularly given the UK's regulatory requirements for 2025. The emphasis was on identifying vulnerabilities and ensuring that these were escalated appropriately to drive prioritisation at senior level. However, attendees raised questions about whether the scenario testing which organisations carried out was severe and realistic enough to evaluate their impact tolerances. One participant said, "regulators expect us to already be resilient," suggesting a gap between expectations and actual readiness.

The panellists agreed that internal audit is taking the auditing of culture and ESG risks more seriously. Culture was described as a business-critical risk, with deep-dive audits increasingly conducted to evaluate behaviours, outcomes, and alignment with organisational values. This work often involved behavioural psychologists and qualitative assessments, presenting challenges for both auditors and stakeholders, as it moved beyond traditional policy-driven audits. "It's far more personal, dealing with behaviours rather than processes," one panellist said. Regarding ESG, the panellists noted its increasing integration into audit functions. While the proportion of time spent auditing ESG risks varied by organisation, public commitments and sustainability policies demand rigorous oversight to manage reputational risks. In addition to climate-related issues, other aspects of ESG – such as diversity and inclusion – were becoming focal points for auditors, particularly in response to regulatory scrutiny.

Participants stressed the need for internal auditors to be outward-looking, engaging with peers across the industry and staying informed about broader market developments. One participant noted, "My driving instructor's term when I was learning to drive, was 'don't be static in the car'. What he was trying to say was, don't just be like, right at this point at this corner, I've got to change gear. I've got to brake. I know, look up. Look around behind you. Look in your mirrors all the time. And I think that's what we need to be doing all the time. As auditors we can't be static in the job." This awareness is essential for maintaining relevance and providing insightful, forward-looking assurance.

An Interview with Tim Peake

1LoD's Editor, Simon Brady interviewed Tim Peake, the first British astronaut to visit the International Space Station (ISS) during XLoD. Tim Peake launched on a Soyuz rocket on 15 December 2015 and landed back on Earth on 18 June 2016, after 186 days in space.

Q: For those members of the audience who are not familiar with your life, could you provide a brief summary of your background, and tell us how you got to where you are now?

Tim Peake: My career as an astronaut started in my mid-30s. Prior to astronaut selection, my background was as a military pilot and actually growing up as a young lad, being an astronaut kind of wasn't on the cards. But for me, being a pilot was my driving passion. I joined the cadets at school and managed to fulfil that ambition of becoming an army pilot quite young in life. Then I went off to the United States and had an exchange tour flying Apaches over there and loved that so much. I came back and wanted to be a test pilot. I spent five years as a test pilot, flying all sorts of aircraft, and then that gave me the skillset really to join the European Space Agency when they had their selection process in 2008 and I subsequently spent 10 years with the space agency, flying the mission as discussed there to the International Space Station for six months.

Q: Those jobs in themselves entailed significant amounts of risk. So how does risk management work in the environments you've just outlined?

Tim Peake: As a test pilot, what we're doing is taking an off-the-shelf piece of equipment and we want it to do more, perhaps more than the manufacturer intended. we'll work very closely with the manufacturers because clearly we have to have an understanding of their product, of what it was designed to do and what they tested it, and that is the same for the audience with their processes and procedures. How far they tested it, how much of that testing was actual testing and how much of it was just extrapolated data on which they don't actually have very firm data points.

By looking at what we wanted to try and achieve, what boundaries we wanted to push, we then developed a test programme involving the experts in an incremental approach just changing one parameter at the time and evaluating that, seeing how we go fully instrumenting

the aircraft. And that's the kind of process we would go trying to mitigate the risk where we see them and then we get in people from other industries who have no idea about aviation because we want to just have that kind of blue skies approach to, OK, what are we missing here? We're all in a bit of an echo chamber. We've peer-reviewed this. We've evaluated all the risk. We've mitigated as much as possible.

Q: This audience will call this risk acceptance. So, have you noticed any differences in the risk processes in, in the military and space agencies and other places you've worked? What are the good and bad bits of that again sort of from your perspective as the person relying on others?

Tim Peake: There are differences. As a military test pilot, you tend to be perhaps in some respects the more comfortable position of being the technical expert. I was probably one of 10 people who knew what the Apache helicopter could do in the world. And so that puts you in a position of firstly, you understand the risk that you're taking because you know that machine intimately, but also it puts you in the position of you being the one who has to fully understand the risk that you're taking, perhaps better than anybody else in the space agencies. We're not trying to push these spacecraft or push the space station beyond the boundaries. We're trying to work within the tolerances with which it was designed, but I don't know it to the same degree that I knew the Apache helicopter. So now you're trusting the organisation, you're trusting the corporate risk and the collaboration around the world of all the quality control systems that go to make that.

Q: If you don't have risk culture correct throughout an organisation you can get silos. You can get people who want to protect themselves, not the mission. Have you encountered sort of bad culture?

Tim Peake: It comes down to understanding the risk culture and having a very clear system of transparency within the organisation that you're working in. Clearly NASA have had several accidents which have transformed the way they operate. But now you have a completely different approach where the two crew members, Butch [Wilmore] and Suni [Williams], were intimately involved in all the decision-making. They had flown that spacecraft to the space station, and they had determined that there had been some anomalies on the way.

Q: In banks, you have the Rainmaker culture, these potentially maverick risk-taking individuals and you know at some point they make an enormous amount of money for the bank. But at the next point on, they're making the money, but they're taking too much risk. Do you see any parallels within your previous experience?

Tim Peake: I think what's interesting is probably some parallels with how the two sides of the organisation work. You know, the special forces would see that risk mitigation process as being bureaucratic, as slowing down the whole process, they need to be more agile, more innovative, they need to have the freedom of flexibility to buy the kit that they want and use it. The key, however, is to keep improving those links, the collaboration, the cooperation. Special forces tend to operate in a silo, and they like that, and they're protected. I think it was just breaking down some of those communication barriers and education.

Q: Is it important that you have fear?

Tim Peake: You do get afraid, and I think that's a good thing. And we do acknowledge that because it's fear that allows us to analyse why are we afraid? What are we afraid of? Can we do something about it? Can we control it? If we can control it, then let's look at what we can do. If we can't control it then that's our residual risk. Then we determine, are we happy as an individual?

Q: Is there a point at which you would have said 'I'm not getting in that Apache helicopter'? I am not sitting on that rocket. I am completely uncomfortable. You haven't delivered to me an organisation which makes me comfortable with the risk you're asking me to take?

Tim Peake: I've never gotten anywhere close to that, but certainly been intimately involved in the loop that tries to establish what exactly is the risk and do we understand the risk and why are we doing this? So as an astronaut you work closely with the industry. And one of the projects I was assigned to was actually looking at Boeing Starliner and doing an independent risk assessment. And we were looking at levels of redundancy with its re-entry.

Q: Would you go to Mars if you were given the chance?

Tim Peake: Not right now. Kind of busy, but no. Mars is going to be a three-year mission. So, it's a long period of time. I think we have to start getting into the mindset that [a long mission] becomes the norm though in the future. It was the norm back in the 1850s with Royal Navy expeditions – three to five years was considered the norm.

Q: At any point during a launch countdown, have you wondered, is this a good idea?

Tim Peake: That's probably why they don't give us a countdown! No, we don't get the countdown. We're just looking at the engine startup sequence, so when everybody outside is seeing this 10…9…8…7…, what we're seeing inside the spacecraft is engine fuel pumps on, engine systems are go, life support systems are working normally, pressurised. And then we go engines to 25%... 50%... 100%. So, we're looking at completely different parameters.

Q: And the first time that you did that, what was that like?

Tim Peake: It's incredible because you've done this a thousand times in the simulator, but it doesn't give you the noise, the vibration, the G-force, and there is so much vibration. This thing goes 9,000,000 horsepower, so you have no idea that you've even left the launchpad. It's only after about 10 seconds when the G-force starts to pick up. That's when you think, OK, we are on our way now.

Q: When you entered space for the first time, what went through your mind?

Tim Peake: I was surprised that nothing had happened! In those thousand times in the simulator, it's a wasted simulator sort of if nothing goes wrong. So something had always gone wrong, and when the engines cut out and we got into space, the three of us in the line looked at each other and thought that was strange, It worked perfectly. But at that point when we first got into space, you know, it was absolutely incredible, I mean, just elated really.

Q: Do you have any rituals before or during your missions?

Tim Peake: No, not really, but others do. Signing the door of the cosmonaut hotel that you stay out at the night before, everybody signs that. You have coins that have to be crushed by the train that drags your rocket to the launchpad, and then you carry those crushed coins in your flight suit to space. You're blessed by the Orthodox priests. We all go [to the bathroom] on the back right tyre of the bus as we're on the way to the launchpad. Apparently, that's what Yuri Gagarin did, and if it went well for Yuri, it's going to go well for you.

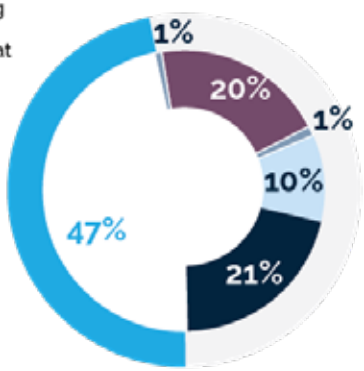
Q: Are there any roles that you regret not taking? Anything you regret looking back that you wish you had done?

Tim Peake: No, I think, I'm very happy how things have worked out. So, in that respect, I am glad that I did stick to my guns as a young pilot in terms of kind of forging that career path that I wanted to take it. Looking back now, I think I'd say to my younger self, you know, have a bit more confidence and stay to what you're passionate about even if it might not seem like the right thing at the time.

Event polls

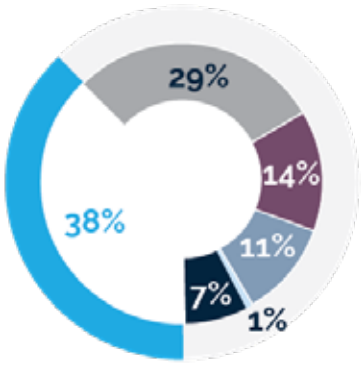
1ST LINE RISK & CONTROL POLL RESULTS

Which Emerging Threat is your highest priority at the moment?

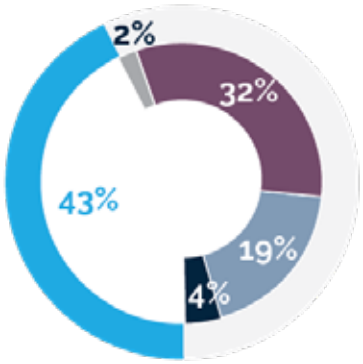


- Cyber / Resilience
- Third Party Risks
- Geopolitical Risks
- Climate Risks
- AI Risks
- Emerging Regulatory Risk

What is your most difficult challenge to overcome when managing emerging threats:

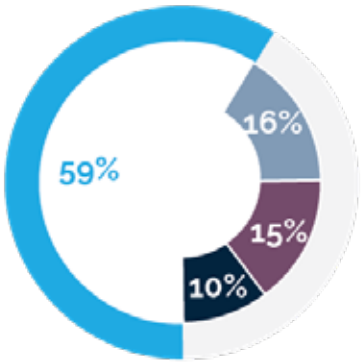


- Lack of Threat Specific Knowledge
- Lack of Resources
- Speed of change
- Dependency on Technology
- Dependency on 3rd Party Vendors
- Heightened Regulatory Expectations



How would you assess the maturity of your 1st line in owning, understanding and addressing the culture and behaviour of their business?

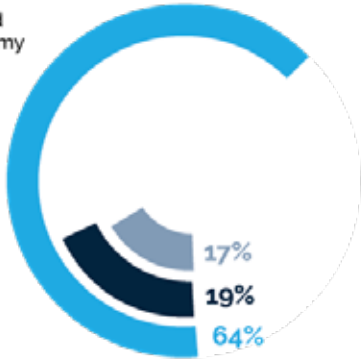
- Sporadic engagement in specific areas, albeit not a consistent priority. Reliance on other functions for cultural work and insights
- Highly advanced, with full ownership, engagement and sophisticated approaches used
- Developing well, with proactive engagement, an acknowledgement of the importance of the topic, and some areas of good practice
- Reactive with limited engagement and understanding, and a heavy reliance on other functions for cultural work and insights
- No meaningful ownership, capability or engagement



What aspect of next-generation RCSAs do you believe will add the most value to your organisation?

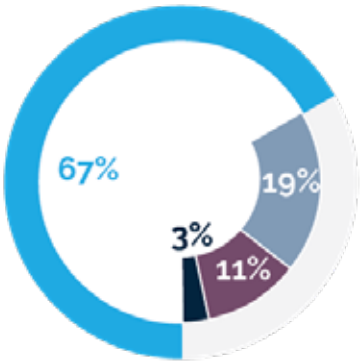
- Real-time risk insights and analytics
- Enhanced automation and AI capabilities
- Improved risk ownership and accountability
- Simplified reporting and compliance processes

The 1st line risk and control function at my organisation:



- Is an effective mitigation for key non-financial risks
- Is an inadequate mitigation for key non-financial risks
- Is an adequate mitigation for key non-financial risks

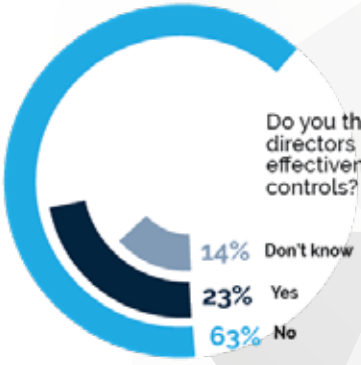
Thinking about the costs of controls, choose the range below which closest describes how much time the 1st line in your firm spends documenting controls/proving that they have controls in place:



What is your primary goal for modernising RCSA processes?

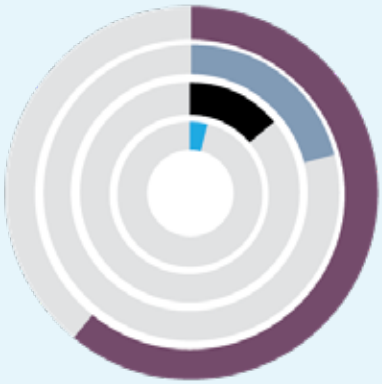
- Gaining more accurate, data-driven insights
- Reducing time and effort in risk assessments
- Enhancing collaboration across functions
- Meeting regulatory demands

Do you think your board of directors understand the effectiveness of your key controls?



REGULATORY COMPLIANCE & MARKET ABUSE POLL RESULTS

What state of detection development is your firm at (pick one):

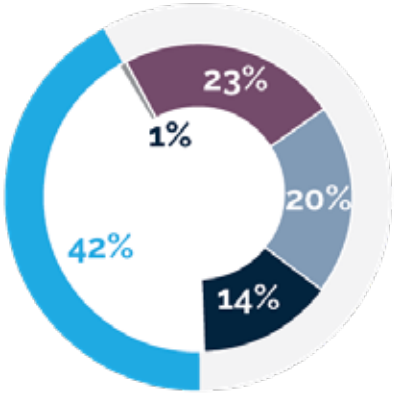


- 61% Lexicon
- 21% In house, supervised model, using logistic regression
- 14% Contextually tuned LLM classifier
- 4% Prompt engineered and weighted GenAI model

My organisation's priority in trade surveillance is:

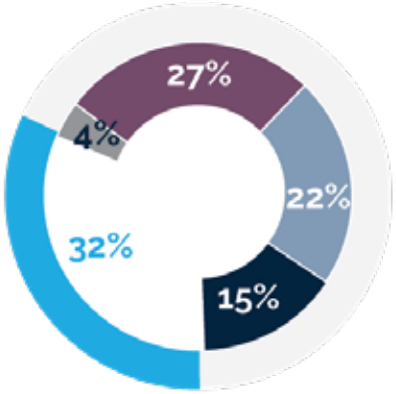
- 35% Ensuring compliance in the wake of recent regulatory enforcements and statements
- 0% Adapting our TS processes to cope with new demands from the business
- 43% Increasing our effectiveness in detecting market abuse
- 22% Increasing the efficiency of our TS processes (e.g. reducing false positives / length of investigations)

How confident are you that your surveillance is capturing all the trading venues used by your front office?



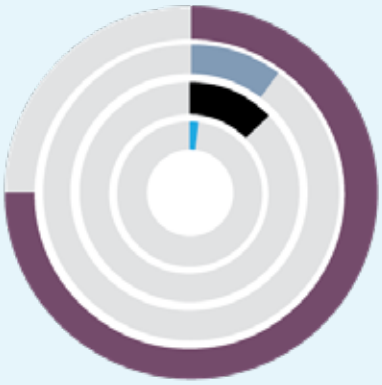
- I am certain that all trading venues are captured
- I am confident that trading venues are captured, with isolated exceptions
- I am certain that many trading venues are not captured
- Don't know
- I am not confident in the level of capture of trading venues, and it is likely there are a number of exceptions

The most promising technology in trade surveillance in the next 18 months will be: (Pick Two)



- Generalised behavioural analytics and signal-based anomaly detection
- Specific trader-based behavioural analytics / profiling
- Improved workflow solutions around investigations
- Integrated solutions for voice, ecomms and trade
- Regulatory data solutions

How confident are you in your firm's communications surveillance policies and their implementation?



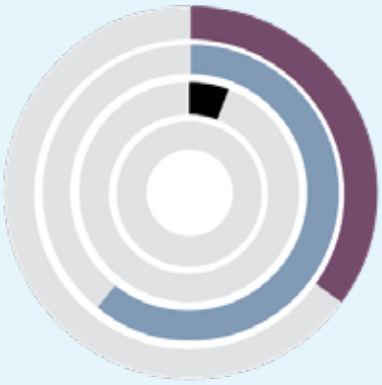
75% Somewhat confident - policies exist but may have gaps or compliance challenges

10% Very confident - comprehensive policies with strong compliance

13% Concerned - significant gaps in either policy coverage or implementation

2% Currently reviewing/updating our policies due to identified weaknesses

How do you expect regulatory enforcement of communications surveillance requirements to trend over the next 12 months?



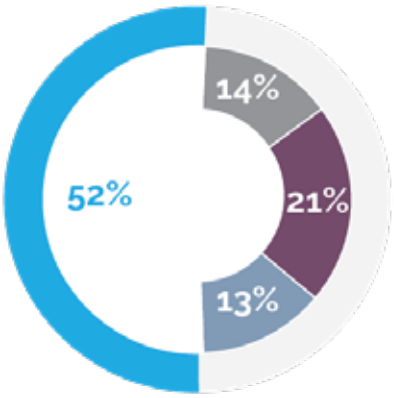
33% Increase significantly - new requirements and stricter enforcement expected

61% Increase moderately - gradual expansion of existing requirements

6% Remain stable at current levels

0% Decrease from current levels

Which statement best describes the maturity of your approach to trading venue governance:



Leading - with all key aspects in place, understood and followed [0%]

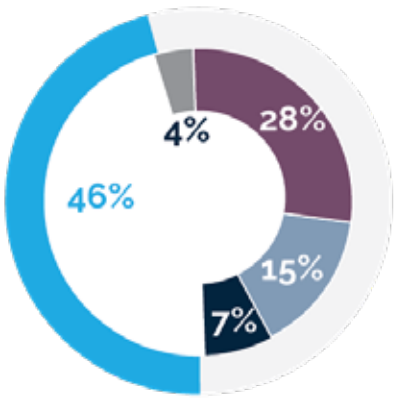
In progress – some areas of good practice, but a number of aspects in development

Well advanced - with only a few areas still to be fully implemented

Immature - with many key aspects not yet in place

Don't know

In the overall Trade Surveillance workflow implemented in your institution, where is AI currently employed (multiple choice):



Data ingestion

Alert generation

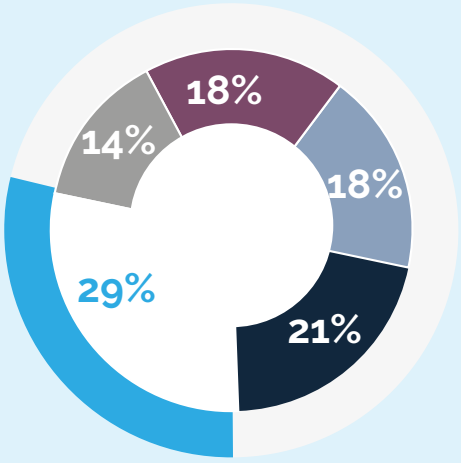
Case management

Rule engine parameterisation fine tuning

Not used

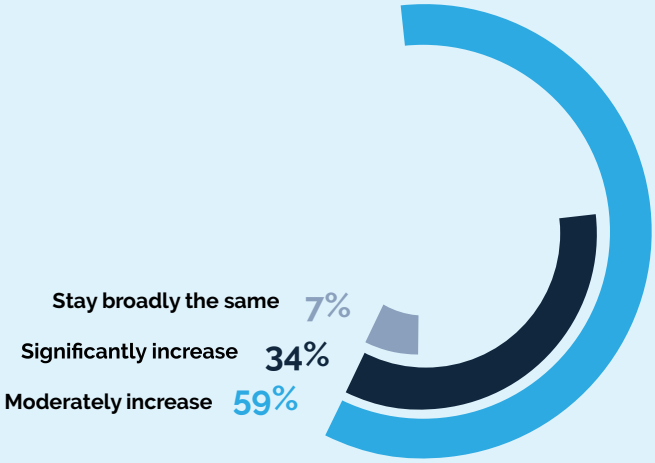
REGULATORY COMPLIANCE & MARKET ABUSE POLL RESULTS

Where is your firm currently when it comes to integrating multiple channels to generate alerts?



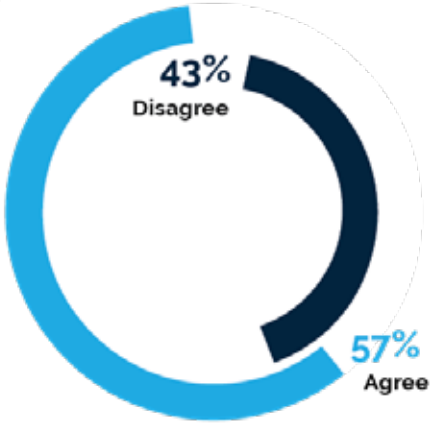
- Not yet considered
- Researching feasibility
- Evaluating vendors
- Actively working on it
- We already run integrated comms surveillance

Over the next 3 years, I anticipate that the in-scope population surveilled by my firm will:

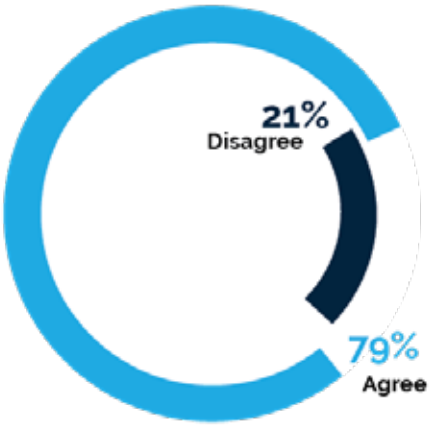


NFR TECHNOLOGY POLL RESULTS

With respect to non-financial risk management, I think my organisational is becoming significantly more innovative:

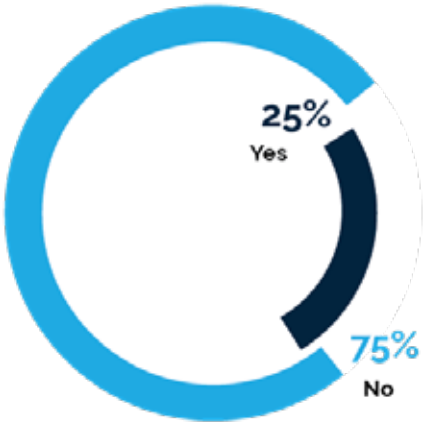


Improvements in transcription accuracy and efficiency are now revolutionary rather than evolutionary:



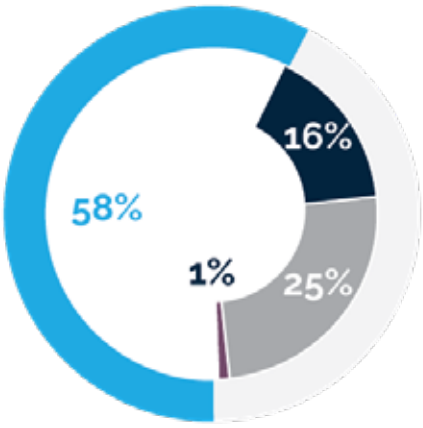
I expect to see a major shift in bank architecture modernisation within:

Are you using AI to improve the quality of your controls?

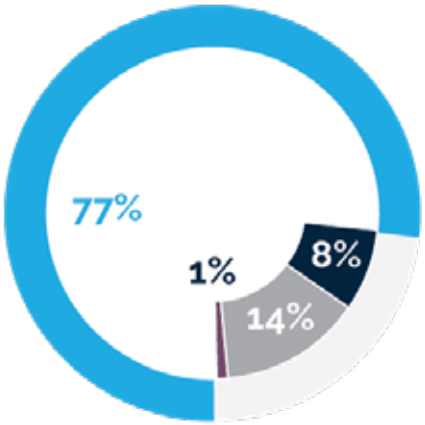


NFR TECHNOLOGY POLL RESULTS

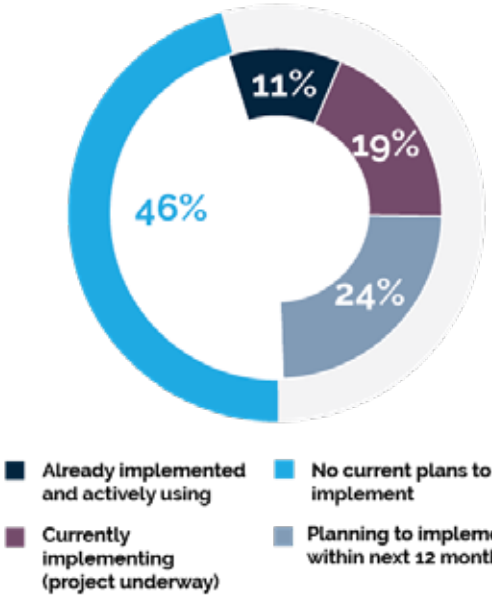
My organisation's technology strategy requires a fundamental overhaul if we are to meet ongoing regulatory requirements in non-financial risk management



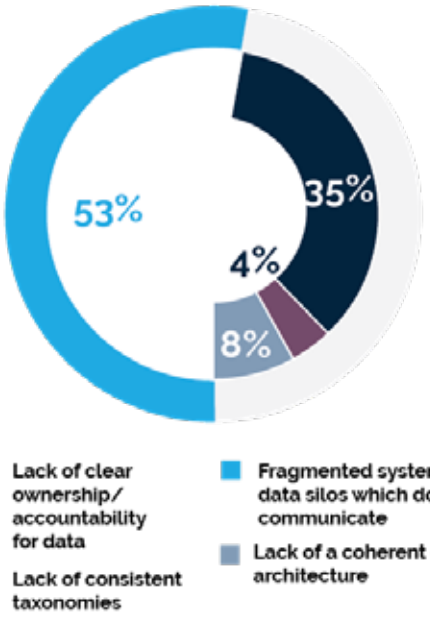
Enterprise technology decisions are taken without sufficient regard for the needs of non-financial risk and control functions



What best describes your firm's implementation of AI or ML in trade surveillance?

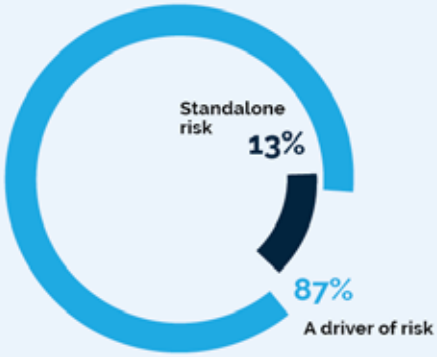


In your firm which of these factors is the most significant root cause of data challenges?

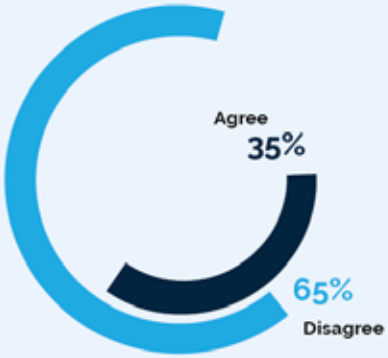


ENTERPRISE RISK MANAGEMENT POLL RESULTS

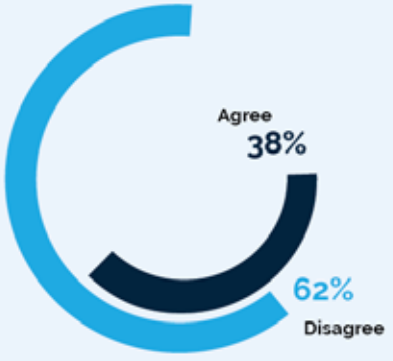
Do you treat geopolitical risk as standalone risk or driver of risk? Choose one of:



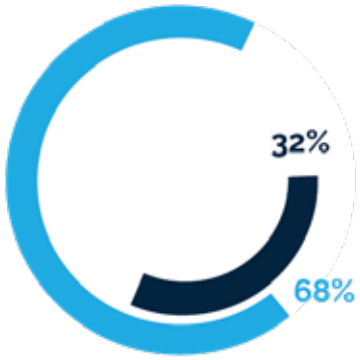
My organisation is not currently planning significant changes in its risk management framework.



My organisation adequately considers the wide range of risks arising from market interconnectivity.



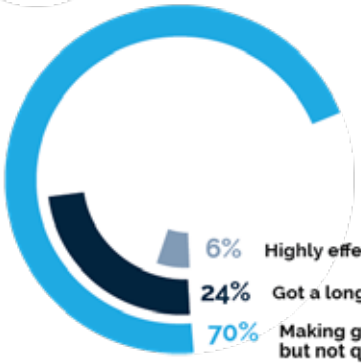
Are regulators a help or a hindrance when it comes to firms' adoption of gen AI tools and solutions?



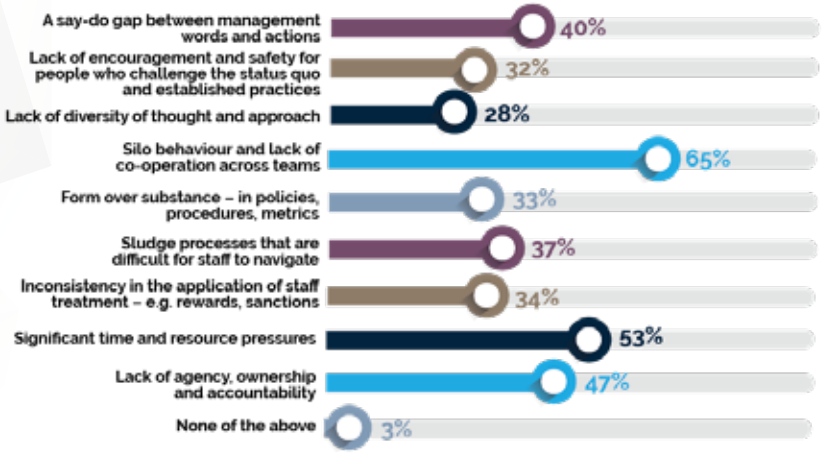
Regulators so far have been more of a hindrance – regulators should give more clarity to firms to reduce regulatory risk and expense for firms in relation to their adoption of gen AI tools and solutions

Overall, regulators' input has been helpful – but clearly there's a lot still up in the air

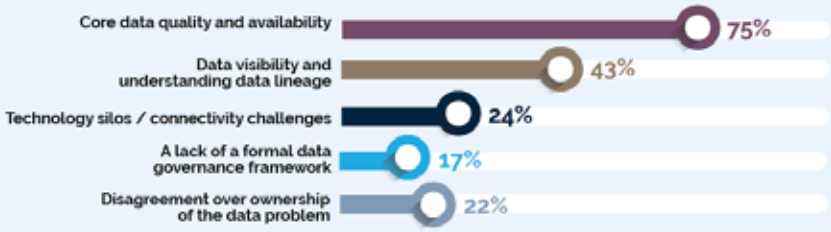
How effectively does your firm address third party risk? Choose one of:



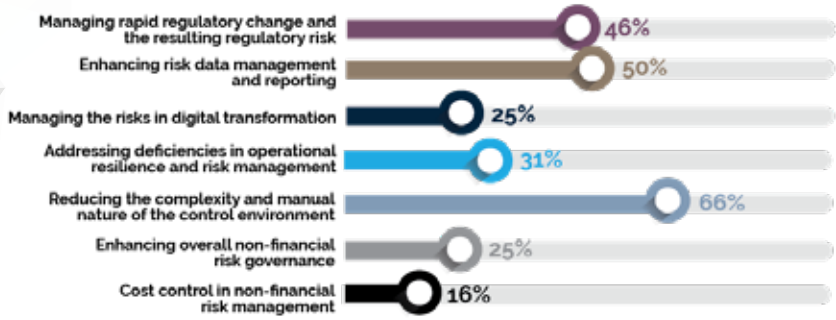
Which of the following cultural challenges are present in your organization? (multiple answers allowed)



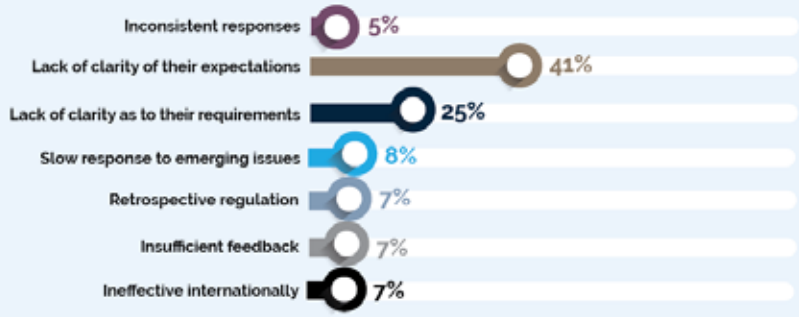
The most significant data issue in my organisation is: (pick the two most important)



What are your key risk and control priorities for 2025 (pick the three most important)

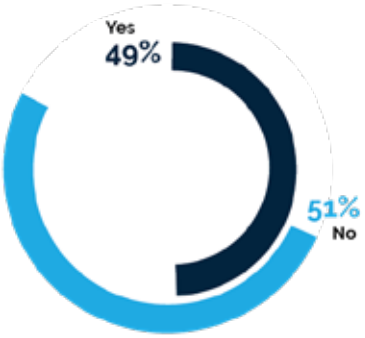


What frustrates you/your firm most about regulators? [pick one]

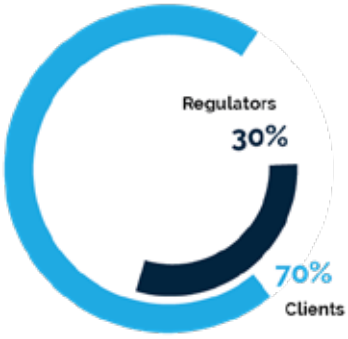


ENTERPRISE RISK MANAGEMENT POLL RESULTS

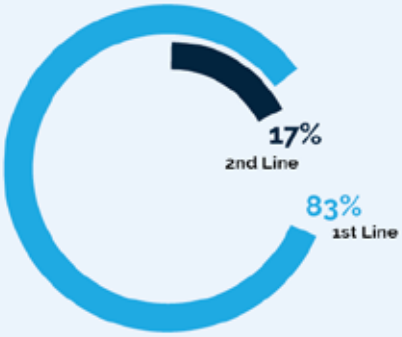
My organisation applies the same systematic NFR risk process to reputational risk as it does to other risk types such as resilience risk and conduct risk:



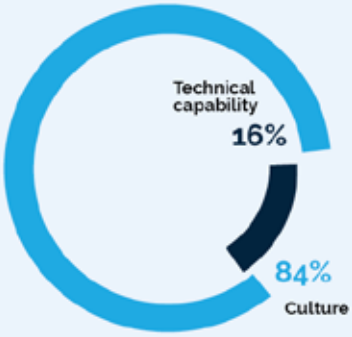
From a reputational perspective it is more important to protect our relationship with:



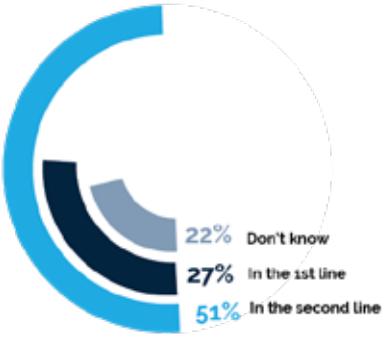
I believe the primary location for Operational Risk Management activities should sit in:



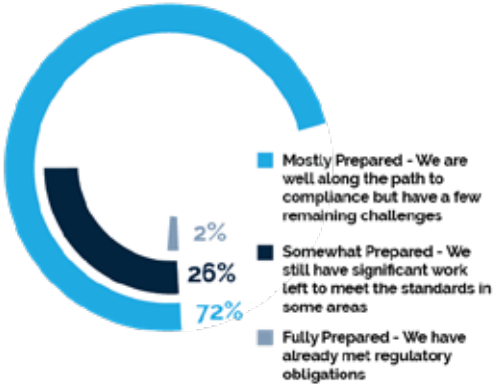
Does culture or technical capability matter more?



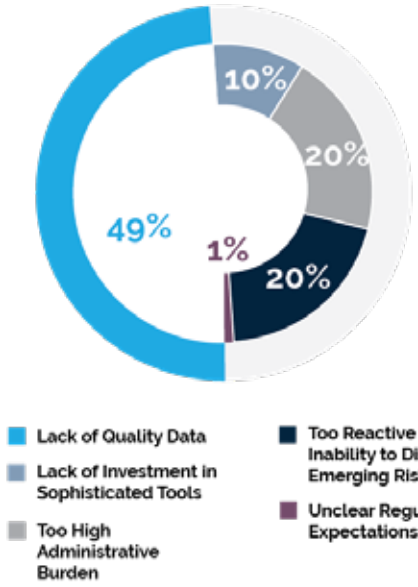
The legal function in my organisation sits:



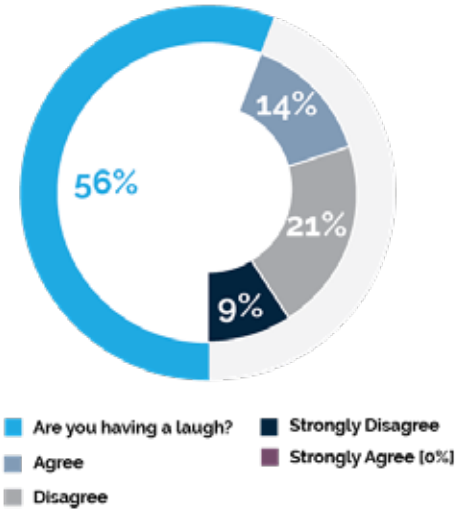
How prepared is your firm for the 2025 operational resilience regulation?



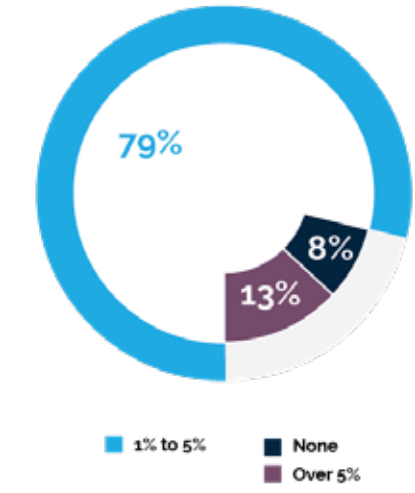
In my firm, the biggest challenge facing more effective Operational Risk Management is:



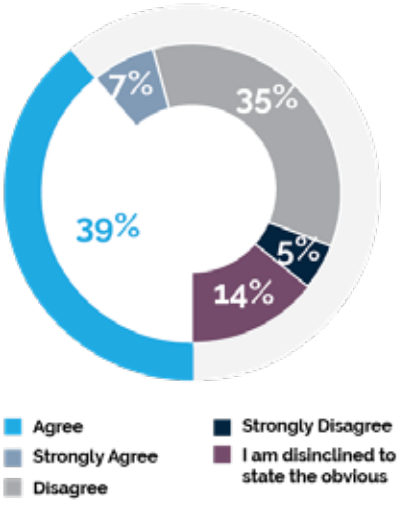
If my life depended on my bank's non-financial risk management processes, I would sleep well at night:



My organisation's internal audit function devotes the following percentage of time to audits of ESG risks:



Banks' commercial and 'rainmaker' culture is antithetical to building a strong, collaborative, compliance and risk management culture:



ENTERPRISE RISK MANAGEMENT POLL RESULTS

What is the most significant outstanding challenge your firm faces in relation to operational resilience in 2025 and beyond?

59% Strengthening 3rd party and supply chain risk management

11% Enhancing scenario testing capabilities

6% Addressing resilience regulatory requirements globally

24% Embedding resilience within BAU operations

From a risk management perspective, how do you rate the clarity of roles and responsibilities across the three lines of defence in your firm?

5% Super clear – all good

45% Pretty good – not perfect, but good enough

45% Really need to make progress, but it's do-able

5% A long way off having the clarity we need – a mountain to climb

The legal function too often takes too conservative an interpretation of regulatory issues:

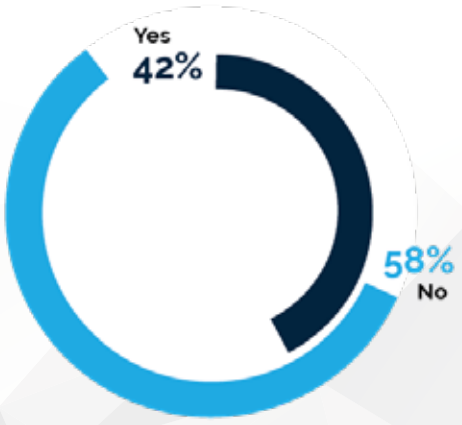
48% Agree

8% Agree Strongly

44% Disagree

0% Disagree Strongly

My organisation's Internal Audit Function is using AI in its audit work?



Join us at XLoD® Global

Innovation & Collaboration: Advancing Non-Financial Risk Management Across the 3 Lines of Defence

NEW YORK	SINGAPORE	LONDON
4 June 2025	24 Sep 2025	11 & 12 Nov 2025

1LoD® 2025

Events, Training and Development Intelligence for Non-Financial Risk and Control Practitioners across the 3 lines of defence

Download the **2025 Group Deals brochure** to secure the best rates of the year for your function. Benefit from a Group Deal to plan a whole year's worth of training and development opportunities for your team globally.

For more details, please contact **Dane Barnard**, Director, Head of Financial Institutions. **Dane.Barnard@1LoD.com**

www.1lod.com/xlod