

A 1LoD report



# The Surveillance LEADERS' NETWORK

FORECAST 2026

February Meeting, London

## The Next Phase of Surveillance Governance, Operating Models, and AI Enablement

Sponsors

BEHAVOX



EVENTUS



INSIGHTFUL  
TECHNOLOGY



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

# The Next Phase of Surveillance Governance, Operating Models, and AI Enablement

“Excellent thought-provoking small group discussion  
allows diverse views to be discussed.”

SIMON FRIEND, MANAGING DIRECTOR EMEA HEAD OF SURVEILLANCE, RBC  
CAPITAL MARKETS

## Key takeaways

01

Surveillance model classification has become a strategic governance lever, directly shaping validation scope, resourcing decisions, and regulatory exposure

02

Artificial Intelligence (AI) adoption in surveillance is accelerating, but testing requirements, model risk expectations, and explainability demands are creating material operational friction

03

The 1st line versus 2nd line debate is increasingly less about structural placement and more about clear accountability, escalation rights, and cultural alignment

04

Communications surveillance is shifting from channel-by-channel monitoring towards multi-channel contextual intelligence, increasingly linked to trade and external datasets

05

Data completeness, connector complexity, and reconciliation controls remain foundational weaknesses that technology alone cannot resolve

06

Human expertise remains essential to ensure AI-enabled detection is meaningful, defensible, and operationally usable, particularly in nuanced behavioural interpretation



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

## Model Governance and Proportionality in an Expanding Risk Framework

A central theme throughout the Network was the increasing formalisation of surveillance model governance. Participants reflected on how regulatory expectations had evolved, particularly as supervisory focus on Model Risk Management (MRM) had expanded beyond front-office pricing and credit models into conduct and market abuse controls. This shift had forced firms to reconsider how they define, classify, validate, and document surveillance tools.

One recurring observation was that regulatory definitions had broadened materially in recent years. As one participant noted, "with the greater use of AI, much more has come into scope in terms of what constitutes a model, significantly expanding the boundaries of model risk management and governance." Tools that were previously considered operational rule engines or configurable thresholds were now subject to formal model governance frameworks. This reclassification had implications not only for documentation but also for validation cycles, independent review, and change management.

However, the discussion did not reflect resistance to governance. Rather, it centred on proportionality. Participants repeatedly emphasised that not all surveillance models carried equivalent risk. Deterministic rules based on regulatory scenarios were qualitatively different from machine learning (ML) algorithms that adapt over time. As one attendee stated, "not every model needs that level of validation", and banks should consider this when grappling with how to calibrate oversight appropriately.

Firms described developing tiered frameworks that distinguish between predictive AI models, behavioural analytics engines, and rules-based alert systems. Higher-risk models incorporating Natural Language Processing (NLP) or behavioural clustering were increasingly subject to more extensive back-testing, bias testing, and performance monitoring. Lower-risk systems could undergo lighter validation focused on logical integrity and calibration effectiveness.

Participants also highlighted a marked shift towards return on investment (ROI) scrutiny. Surveillance funding now competed with wider AI initiatives and business expansion programmes, meaning regulatory necessity alone was no longer sufficient justification. As one contributor stated, "it's about the ROI now...your case studies have to show 'I can generate X times that return on investment' to actually get the funding over the line." Investment



**“Great insights and a good way to keep with the new themes and challenges in surveillance.”**

**HAMMAD HANIF, HEAD OF TRADE SURVEILLANCE AND BENCHMARK MONITORING, LLOYDS BANKING GROUP**

cases had to demonstrate measurable value, not just compliance alignment. Articulating that value was challenging. Avoided fines were hypothetical until enforcement occurred, and as one participant noted, momentum often accelerated only once firms were "slapped with this proverbial Matter Requiring Attention (MRA)." Others emphasised operational benefit, arguing that "when you have better tools, you need less people, you have better results." However, the debate extended beyond headcount reduction to prioritisation and sustainability, including consideration of "the total cost of ownership and the cost of change."

Cross-functional collaboration was identified as critical to making these frameworks workable. Surveillance teams could not govern AI in isolation. Engagement with data science, compliance, technology, and MRM functions early in the development lifecycle was described as essential to avoid late-stage validation bottlenecks. At the same time, several participants observed that ultimate accountability often rested with surveillance, even after validation approval. This reinforced the importance of robust internal challenge and documentation ownership.

The validation of AI-enhanced communications models generated particular debate. Some firms reported extensive testing regimes requiring

thousands of sample inputs before approval. Others described inconsistencies in how validation standards were applied across communications and trade models. The result was an environment where governance expectations could feel uneven, particularly where validators had limited familiarity with surveillance methodologies.

Documentation and auditability emerged as non-negotiable pillars of defensibility. Regulators increasingly expected a consolidated narrative explaining model purpose, design choices, data inputs, threshold rationale, tuning decisions, and performance metrics. Firms reported investing in centralised documentation repositories and structured change management logs to ensure traceability. The underlying message was clear: effective surveillance governance was no longer an informal operational discipline but an embedded component of enterprise model risk architecture.

Looking forward, participants anticipated continued regulatory focus on explainability, bias risk, and ongoing performance monitoring. Governance therefore had to evolve in parallel with technological capability. The next phase would require surveillance functions to combine analytical sophistication with disciplined control frameworks that withstand regulatory scrutiny without paralysing innovation.



**Subscribe here**

to receive new content  
and event information  
directly to your inbox

# Operating Model Design and the Reality of Accountability

The longstanding debate over whether surveillance should sit in the 1st line or 2nd line featured prominently, yet discussions quickly moved beyond structural orthodoxy. Participants suggested that the effectiveness of a surveillance operating model depended less on formal line designation and more on clearly defined accountability, independence safeguards, and escalation pathways.

Some firms had transitioned between models, experimenting with fully embedded 1st line surveillance teams before shifting oversight responsibilities to the 2nd line, or vice versa. These experiences revealed that structural relocation alone did not resolve tensions around independence or business proximity. As one participant recounted regarding regulatory engagement, supervisors "could not care less" about where surveillance sat, and what got regulators comfortable was "having clear policies and procedures in place to evidence that there is no conflict".

The historical roots of the debate were described as centred on reporting lines and remuneration authority. Questions such as who approved budgets, who conducted performance reviews, and who had authority to escalate concerns remained fundamental to independence. Participants emphasised that governance documentation, formal escalation rights, and transparent oversight committees often provided stronger safeguards than positional separation alone.

The allocation of tasks across the alert lifecycle was explored in detail. Many firms operated hybrid arrangements in which L1 triage sat close to the





business to maintain contextual awareness, while L2 investigation and thematic oversight remained within a more independent function. Others centralised investigation entirely but maintained strong oversight by risk committees. The key requirement identified was clarity. Every stage from alert generation to reporting had to have defined ownership and documented escalation triggers.

Cultural dynamics were repeatedly cited as decisive. As one participant stated succinctly, "it is all about culture and removing the stigma tied to the different lines of defence" with another participant adding "if more effort was made to engage with both the 1st and 2nd lines it would not matter where surveillance sat." Surveillance effectiveness depended on the willingness of trading desks and business leaders to engage constructively with oversight, participants agreed. Where surveillance was perceived as adversarial or disconnected, cooperation could diminish. Conversely, excessive proximity risked blurring lines of independence.

Several contributors challenged the rigidity of the traditional 3 lines construct. One comment captured this frustration: "the whole lines of defence concept, it gets in the way." As surveillance increasingly overlapped with financial crime monitoring, transaction monitoring (TM), and conduct risk analytics, the boundaries between control functions were becoming less distinct. Firms were therefore experimenting with integrated surveillance ecosystems supported by shared data infrastructure and common investigative tooling.

Ultimately, the consensus was pragmatic. The most effective operating models were those that clearly defined accountability, ensured independence in decision-making, and maintained sufficient proximity to understand evolving trading behaviours. Line placement was a design choice; accountability and governance discipline were non-negotiable.

## AI-Enabled Communications Surveillance and the Data Challenge

AI dominated discussions on the future of communications surveillance, with participants describing rapid improvements in transcription, translation, and behavioural analytics. One attendee characterised recent advancements as a "hockey stick of explosion" in capability. Yet alongside optimism came sober recognition of persistent technical and operational limitations.

Language detection and code switching were repeatedly identified as complex challenges. Employees often switched languages mid-conversation or incorporate colloquialisms that confuse automated systems. Participants explained that many platforms still scored language "on the chat level, as opposed to message-to-message level." This limitation could misclassify multilingual exchanges, affecting downstream detection logic.

Nuance and context remained equally problematic. Straight translation did not always capture intent, particularly when non-native speakers used idiomatic expressions. Firms described instances where escalations triggered by automated analysis were later deemed benign upon closer cultural review. These experiences

The "human-centric contribution" was described as indispensable, particularly in reviewing complex behavioural anomalies.

reinforced that AI could not yet replace human judgement in behavioural interpretation.

The conversation moved towards integration and contextual analytics. Participants articulated a future state in which communications, voice transcripts, and trade lifecycle data were linked within unified investigative platforms. One attendee warned that without integration teams might fail to "pull together that scene," potentially missing distributed risk signals. Multi-channel analysis promised richer insight but required substantial data engineering investment.

Data governance emerged as a critical enabler. Participants reported managing hundreds of data connectors and grappling with unsupported communication platforms, including encrypted messaging tools. Reconciliation processes, feed monitoring, and vendor oversight were described as increasingly resource-intensive. Surveillance teams often found themselves performing data management functions traditionally owned by technology or IT departments.

AI adoption also raised questions about workflow design. Some systems now auto-closed lower-risk alerts with documented rationale, while investigators focused on higher-risk cases.

However, participants cautioned that optimisation could generate new detection volumes, requiring careful resource planning. The "human-centric contribution" was described as indispensable, particularly in reviewing complex behavioural anomalies.

Regulatory scrutiny continued to intensify alongside technological innovation. Supervisors were requesting evidence of language coverage, detection accuracy, and completeness of record capture. Firms had been asked to demonstrate the languages actively used by trading populations and justify monitoring strategies accordingly. This reinforced the importance of defensible methodology and transparent reporting.

Looking ahead three to five years, participants anticipated greater convergence between AI-enabled surveillance and behavioural risk analytics. Anomaly detection, contextual linking, and integrated dashboards would likely become standard components of modern surveillance ecosystems. However, sustained investment in data integrity, explainability, and governance discipline would determine whether technological promise translated into durable risk reduction.

**This information was taken from the  
Surveillance Leaders' Network meeting  
in London on 12 February 2026**

# 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

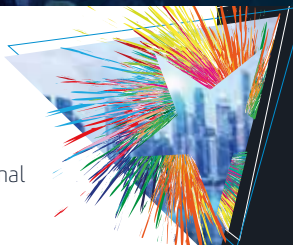
XLoD Global  
An in-person conference

[www.1lod.com](http://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

