

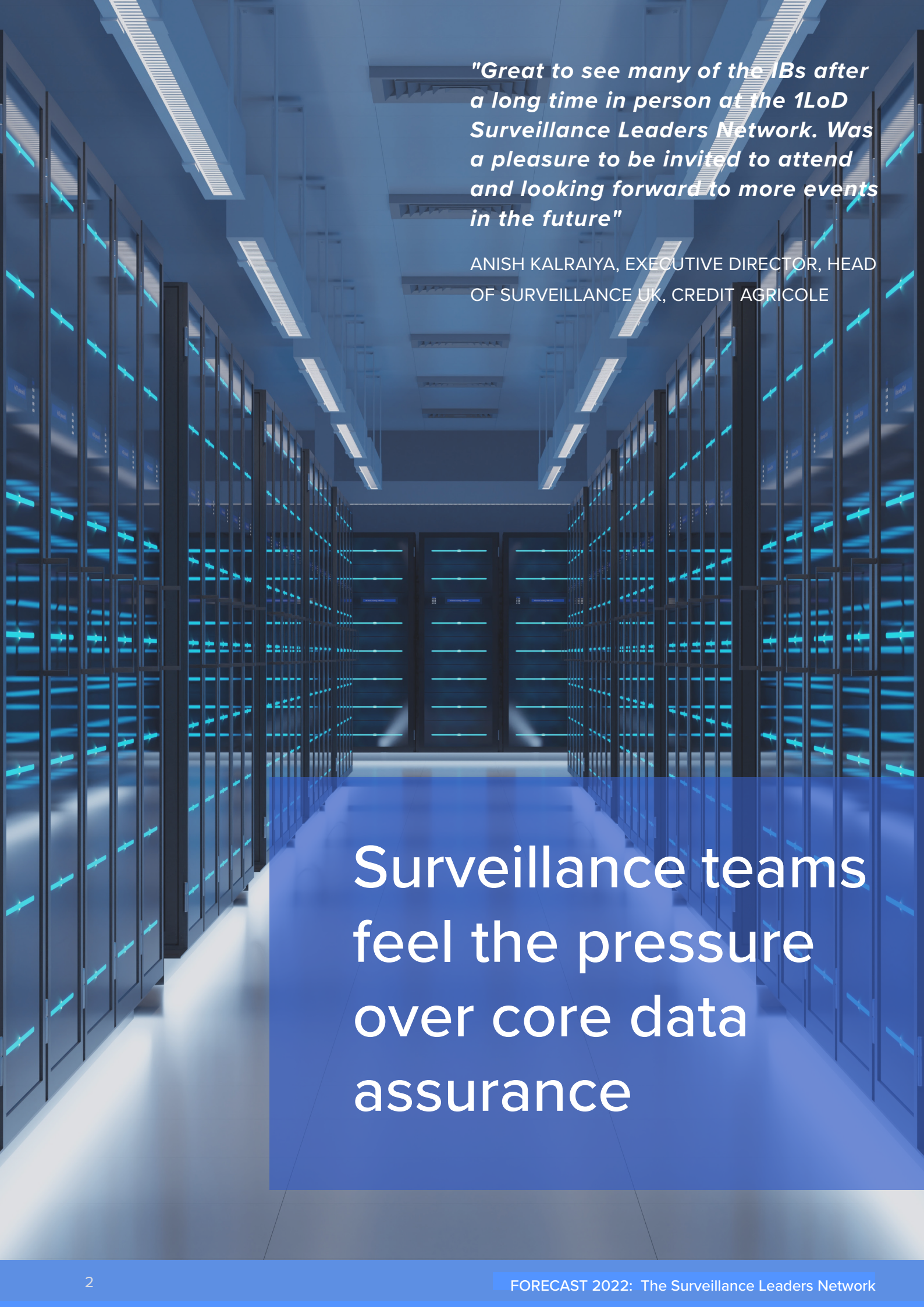
The background of the entire page is a dark, futuristic office or server room. The ceiling is dark with recessed rectangular lights. On the right side, there are rows of server racks with glowing blue and purple lights. In the center and left, several human figures are depicted as glowing blue wireframe or particle-based models. One figure in the center is holding a tablet. To the left, there are desks with computer monitors displaying blue data. The overall atmosphere is high-tech and digital.

smarsh®

1LoD®

THE SURVEILLANCE LEADERS NETWORK

FORECAST 2022



"Great to see many of the IBs after a long time in person at the 1LoD Surveillance Leaders Network. Was a pleasure to be invited to attend and looking forward to more events in the future"

ANISH KALRAIYA, EXECUTIVE DIRECTOR, HEAD OF SURVEILLANCE UK, CREDIT AGRICOLE

Surveillance teams
feel the pressure
over core data
assurance

Key takeaways

- A back to basics approach-to-data assurance – capture, storage, indexing – is overdue
- Regulatory focus on data completeness and immutability is a game changer
- Many voice and other data capture platforms are still too inaccurate
- Surveillance data and applications should move from on premises to the cloud
- Using outdated on-premises security and privacy controls is delaying cloud implementation
- Fines for cross-product fixed income abuse mark a turning point for surveillance teams
- New approaches in data and tech are needed in complex markets such as fixed income
- Surveillance systems designed for listed equities may not satisfy regulators in other markets

Recent US enforcement actions have highlighted the difficulties banks face in surveilling the communications channels and asset classes regulators demand. The fines reveal failings across the surveillance process, from data capture to overall culture, and emphasize that skimping on surveillance is a false economy. The time for tweaking is over: it is imperative that banks make significant investments in data assurance, increase their monitoring of known channels of communication and commit to detecting abuse in complex markets.

The recent JP Morgan and NatWest fines resulting from US Department of Justice (DoJ) action were key conversation topics at the latest 1LoD Surveillance Leaders Network, held in-person in London. It is clear that regulators now expect banks to resolve the long-standing difficulties associated with recording communications and keeping records, and to cover all regulated activity, regardless of the communications channels used. Regulators also expect banks to be able to detect misconduct not only in liquid, listed assets such as equities, but also in more complex types of asset, notably fixed income, where simply detecting anomalous trades in individual securities is not enough.

New data paradigm needed

The foundation of any surveillance operation is the ability to capture and index the data related to regulated activity in such a way that it can be retrieved and analysed. This presupposes that banks can identify the communications channels used by regulated persons and record them, and the trade data associated with their activity.

But, as the practitioners at the event agreed, there are significant problems with all of those assumptions. Banks cannot guarantee to identify every communication channel used by their traders. Take the example which came up in discussion: A trading venue rolled out a new chat functionality 6 months after going live with its trading platform, but because nobody in the business had told the compliance division about this, its content was not included in the bank's surveillance programme for several months. Surveillance functions struggle to record the channels that they do know about (the obvious ones being messaging apps and some of the communications options embedded in collaboration applications such as Teams, Zoom and Slack), and cannot definitively cover those used on personal devices such as phones and tablets which were prevalent even before the pandemic and which have become ubiquitous in the era of hybrid working.

Participants expressed particular concerns about voice channels. Asked whether their firm's voice surveillance programme is now as effective as the e-comms surveillance programme, only 35% agreed.

[\[chart 1\]](#)

Voice channels present several challenges when it comes to surveillance. There is the issue of voice-to-text transcription, the accuracy of phonetic lexicons, the nascent state of artificial intelligence (AI) and natural language processing (NLP) analytics, and the difficulty of multi-lingual coverage. However, attendees identified much more fundamental problems.

As one participant explained: "Because of shortcomings in voice-recording solutions, you can easily miss between 5% and 30% of the call data. Also, some recording systems have a maximum length of call recordings before they cut and maybe start again. So, if you don't know that that call was over a particular length of time, you might only be looking at the first half. You don't even know that there's the second piece there. It's very, very important to be aware of the exact recording limitations of your particular solutions.

"All of these issues lead to a fundamental challenge of basic data assurance. Are banks recording everything they think that they are recording in terms of both voice and other data? Can they prove it? And can they prove that the data is available and has not been tampered with? This last point – data immutability – is critical and is getting the attention of regulators, especially in the light of BS 10008 this is the British Standard which outlines best practice for the implementation and operation of electronic information management systems and, in particular, the need to demonstrate that all electronic records are verified and accessible.

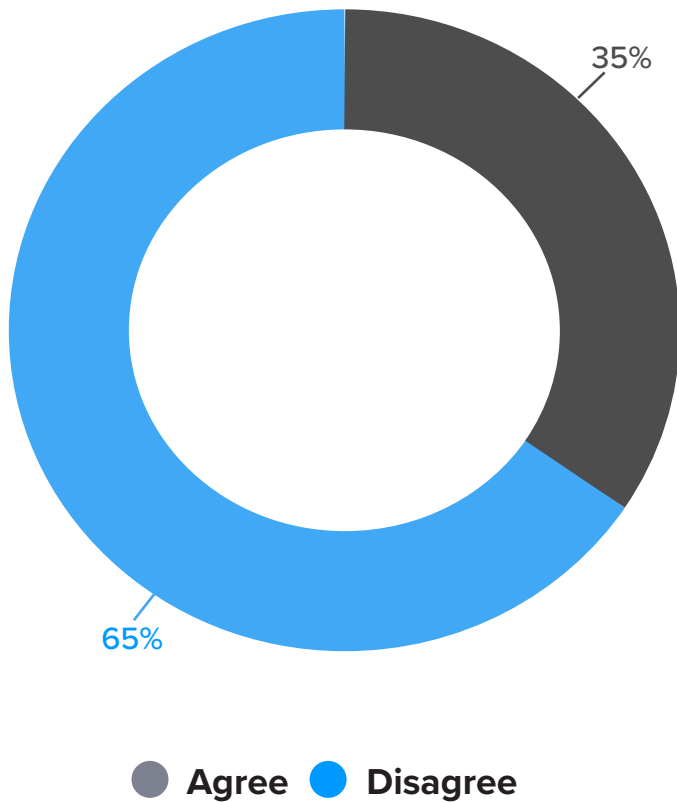
"The implications of data assurance are only just starting to be understood and they are huge," says Rob Houghton, founder and CTO of Insightful Technology. "It's amazing in this day and age, how many voice and other data recording platforms still don't capture everything on a regular basis. The regulators have only just begun to cotton on to this – they didn't used to ask sophisticated questions around data capture and storage – but they're now beginning to understand that there is data missing and that it's because of the way banks' entire capturing and archiving processes work. There are lots of issues but to mention just one: we very often find that the ownership of who's doing the capturing is very different from those who are driving the models and what business requirements are. Before most businesses jump into any future compliance requirements/fulfilment requirements a full discussion and understanding by all parties in what do I have today and what am I going to need tomorrow."

Plugging the gaps with cloud

None of these issues are new, but with regulators clearly in no mood to extend any leeway to new communications channels, personal devices or any other hard-to-monitor risks, banks must now devote time and money to plugging the holes. So, what do they think they need to do?

The most obvious starting point is the problem of core data assurance and that, in turn, begins with data capture. As one participant said: "We all need to recognise that we're not just detecting risk, we're all now running giant data businesses and that, I think, really points us towards having to do things that are outside the traditional surveillance remit."

Chart 1: My firm's voice surveillance programme is now as effective as our e-comms surveillance programme:



"Another informative debate, and it was great to be able to meet some new faces in person. These events really facilitate thought leadership in the field of surveillance."

SIMON FRIEND, HEAD OF SURVEILLANCE, EUROPE AND ASIA PACIFIC, RBC

Several attendees mentioned cloud migration as a potential solution, even though it comes with its own risks. The cloud, in theory, allows banks to deconstruct the silos and processes that are inherent in their legacy on-premises storage. Migration to a single, central cloud data platform also provides a chance to build a metadata capture, storage and indexing facility from scratch, given that metadata is crucial to many of the next-generation surveillance solutions now coming to market.

On the other hand, there are challenges in the Cloud around data protection and privacy, and as Paul Taylor, Senior Director, Solutions Architecture from Smarsh explained, those concerns can get in the way of deployment: "All of our customers are looking at Cloud, but the level of due diligence that we're having to go through to get the approvals to move to Cloud is significant. It's almost the inverse of when we were deploying to on-prem, where we get the approvals reasonably quickly and then it would take a very long time to deploy. Now we can deploy within days, but the actual approvals to be able to push data to Cloud is taking a long time. The issue is that the complexity of the security questions arise because banks often try to map their old on-prem requirements to SaaS or Cloud environments. Vendors need to help them through that process, but I think we all need to understand that Cloud migration is not just as simple as pressing a button."

Practitioners agreed. Several said that they required better processes for IT to bring on board the tools they need, especially for recording.

Dealing with approved channels

Cloud migration can only help with data assurance if the right data is being ingested. But even within approved devices and applications, banks struggle to document all of the communications channels being used by their staff. One participant admitted, “As a surveillance head I struggle to understand what channels are coming into the firm, and by whom, and when, and what are the gateways we have in place to identify those channels. We all know about the problem of employees using communications channels that are not supported by the firm, but that is a whole different conversation.”

Compliance can solve such problems in various ways: by keeping a register of who is using which particular channels within the bank; by using a monthly attestation process and/or governance forum in which businesses formally state which channels they are using; by adding management information (MI) and analytics to avoid reliance solely on attestation; and by incorporating systems and channel inventories into the risk assessment process. This is already revealing systems with communications capabilities that compliance knew nothing about and is helping to drive a cultural change in terms of engagement with the 1st line.

“There were a lot of people who proactively raised their hands and identified systems that surprisingly had communications capability that weren't picked up previously,” said one attendee. “I also think the regulatory pressure sparked a positive move in engagement with the business. A lot of the time previously we struggled to make sure that all the communications were recorded. Now, especially after FCA Market Watch 68, I see a shift where the business is proactively coming to surveillance and saying, “Can I please make sure that your systems are capturing this, this and this system?”

Banks are also increasing their surveillance of the known channels. This means revising lexicons and changing thresholds and parameters so that alert volumes increase which, in turn, means that bigger teams will be necessary to cope with the higher volumes and investment in surveillance will have to rise. The scale of the fines makes the business case easier than perhaps it was.

This should also lead to greater use of automation and more investment in workflow and dashboard solutions that provide analysts with the context for alerts and allow them to process those alerts faster. However, as one participant pointed out, given the time that it takes to bring new technology on board, the increase in workload cannot be reduced in this way immediately: “Especially for large banks, you can't do that [onboard new tech] very easily. It's a year-plus minimum. So, it's not that we don't want to automate, it's just that it would take a long time to achieve. There is also another point: you have to be able to show the regulator what you would do if that automation vendor went down – what's going to be your strategy to get back up and running immediately? – and that same ‘time to onboard’ issue comes up again.”

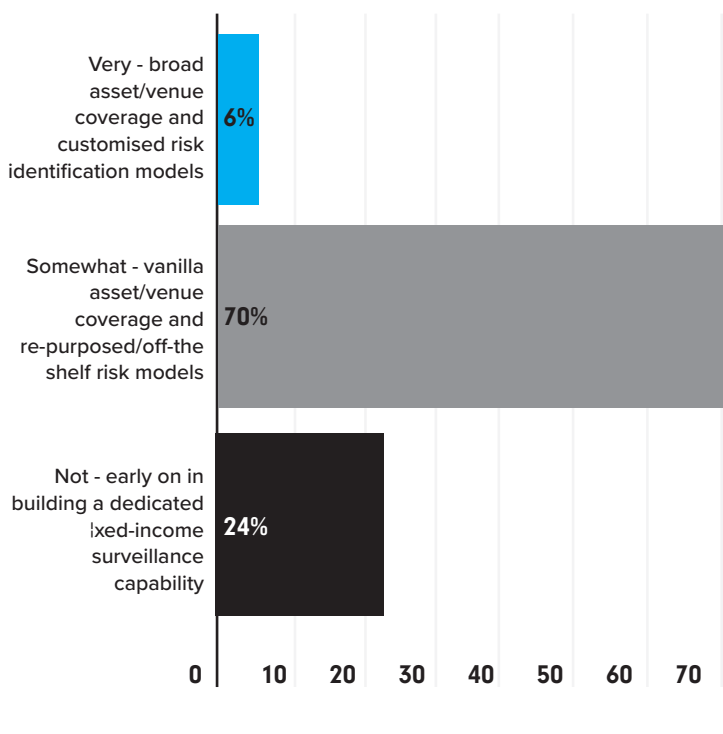
If banks can capture and analyse the communications channels embedded in approved tools, and if the business can help to identify new, unknown channels, then most of the current gaps in coverage will be closed. Personal devices which are allowed and used in the workplace (thanks to BYOD, or bring your own device, policies) remain a significant risk. Even though they may have secure corporate applications installed on them, most attendees agreed that the only solution would be to ban them. But this would relegate them to the shadow world of unapproved channels – and for now, no one has a solution to that problem.

Covering complex assets

In addition to data assurance and channel coverage, the recent regulatory actions by the DoJ also highlighted the challenge of detecting misconduct in markets where cross-asset and correlation trading are the norm, rather than simply taking long or short positions in single securities. The most obvious example is fixed income, where traders and desks think about their overall rate, spread or curve risk across a portfolio of offsetting positions in the cash and derivatives markets, rather than just a long or short equity position.

Market participants acknowledge that their surveillance programmes need more work. Only 6% agreed that their fixed income surveillance programmes had broad asset/venue coverage and customised risk identification models [chart 2].

Chart 2: How mature is your fixed income surveillance programme



NatWest’s recent \$35 million fine in the US, which was for cross-asset spoofing, is proof that regulators now expect banks to pick up on the cross-asset class implications of fixed income. The DoJ was willing to initiate a criminal prosecution in a case in which manipulation of one asset was undertaken to move the price of a correlated asset – and hence the spread between the two – an area which few banks are able to monitor effectively for now.

The implications of this are clear, as Prasad Shinde, Senior Banking & Markets Consultant, KX pointed out. “As the recent fines for spoofing across markets have shown, pre-execution dealing process and cross product/venue activity are firmly in regulatory focus. Surveillance teams need a line of sight on Request for Quotes (RFQs) and the order handling process to identify potential misconduct. They need to be able to visualise price action across venues to a) spot imbalances across orderbooks and b) if any or where traders have placed orders in one venue/related product to affect the price in another. They also need to be able to determine which amongst a multitude of securities might be used as a proxy to affect the underlying price. Using risk vectors & sensitivities will result in a common identifying thread across products and will help teams to effectively monitor misconduct across complex markets.

However, for many attendees, key issues included understanding how to surveil against yield spreads to the reference bond to make comparisons between instruments of different maturities, and even simply understanding price discovery. In request for quote, or RFQ, markets and especially in illiquid and structured markets, surveillance staff may struggle to demonstrate how a particular price was formed and whether it was acceptable at the time. Traders are reluctant to document in detail how price formation occurred, making the subtler discussions of whether a particular trade was used to manipulate an overall risk position irrelevant.

More broadly, surveillance leaders returned to the topic of data capture and record-keeping as unsolved problems in fixed income that should be given priority over smarter analytics. “The biggest challenge we have in this space is just making sure we actually have the data for us to do what we need to do in terms of surveillance and running the models,” said one surveillance head. “The decentralised nature of the marketplace is where the challenge lies – for example, here are these problems with web-based platforms where orders are being placed – and we just need to make sure we can get ahead of that. And some of this is not just a surveillance problem, but also a recordkeeping obligation problem.”

Adapting tech to new markets

Assuming the data is available, banks have another problem in fixed income and other more complex markets. While the traditional platforms, which came out of systems designed for liquid, listed equities, have been adding fixed income models and alerting to their systems, some banks feel that these are not flexible enough to cope with the kind of monitoring that regulators expect.

As Mike Coats, CTO, TradingHub, explains: “Surveillance is the art of understanding the evolution of someone's position around some order book activity and deciding whether it is suspicious in some way. So, you need a framework to understand what position the trader was running. If you ask most fixed income traders about their positions, they wouldn't list their bond inventory, because that wouldn't help them understand the risk they'd taken. They would say I'm long or short duration or convexity; they might say something about where that long/short was most pronounced – “I'm longest at the nine-year point,”; they might describe a curve-steepening position. So, unless you understand that and think like that, then it's very hard to say whether or not

any trade they might have put on is fair or is misconduct of some kind. This means systems which are based very much around individual equity securities and you take the notional and you multiply it by the change in price don't translate easily into fixed income because it doesn't match the way that fixed income traders and risk-managers behave.”

Participants who were unhappy about using traditional surveillance systems, however adapted, were split between adopting sophisticated third-party solutions, often designed by former fixed income traders, and build-your-own solutions. Several attendees said they were developing in-house solutions. One said: “We've gone 90% in-house and we're going to look to eventually phase the vendor solution out and just go completely in-house. The advantage is that you're in control of your own data; you build the models exactly how your business operates; and you can understand the connection between the data that is being ingested and the alerts that are coming out – which is not true if you use some third-party solutions. It also makes calibration and analytics changes much easier.

“Surveillance is the art of understanding the evolution of someone's position around some order book activity and deciding whether it is suspicious in some way. So, you need a framework to understand what position the trader was running. If you ask most fixed income traders about their positions, they wouldn't list their bond inventory, because that wouldn't help them understand the risk they'd taken.”

Building cross-functional teams

Technology is not the only solution. Getting more 1st line expertise into surveillance is one key to understanding the types of market abuse that can happen in complicated asset classes. Working more closely with the 1st line chief operating office can also give surveillance staff access to trader P&Ls to identify unusual movements. Surveillance can then triage those findings with operations staff, product control and risk to see whether they are happy with the activity or not and to give supervisors the confidence that they understand the trading. Documenting that process of collaboration gives additional comfort that regulatory expectations are being met.

Taking this idea of collaboration to its logical conclusion, one surveillance leader said: “I think the days of having your equities trade surveillance team, your FX surveillance team, your fixed income surveillance, may be coming to an end. We are building out a European hub and the teams are smaller, and they cover everything. So, we’ve been really focused on ensuring teams are now a lot more cross-functional, and that allows us to develop that cross-product understanding and also consistency across the board that you need.

“Excellent and informative.”

PAUL DENTON, EMEA HEAD OF COMPLIANCE
SURVEILLANCE, BNY MELLON





Find out more about upcoming events and browse
1LoD Knowledge Hub for the latest insights.

www.1LoD.com