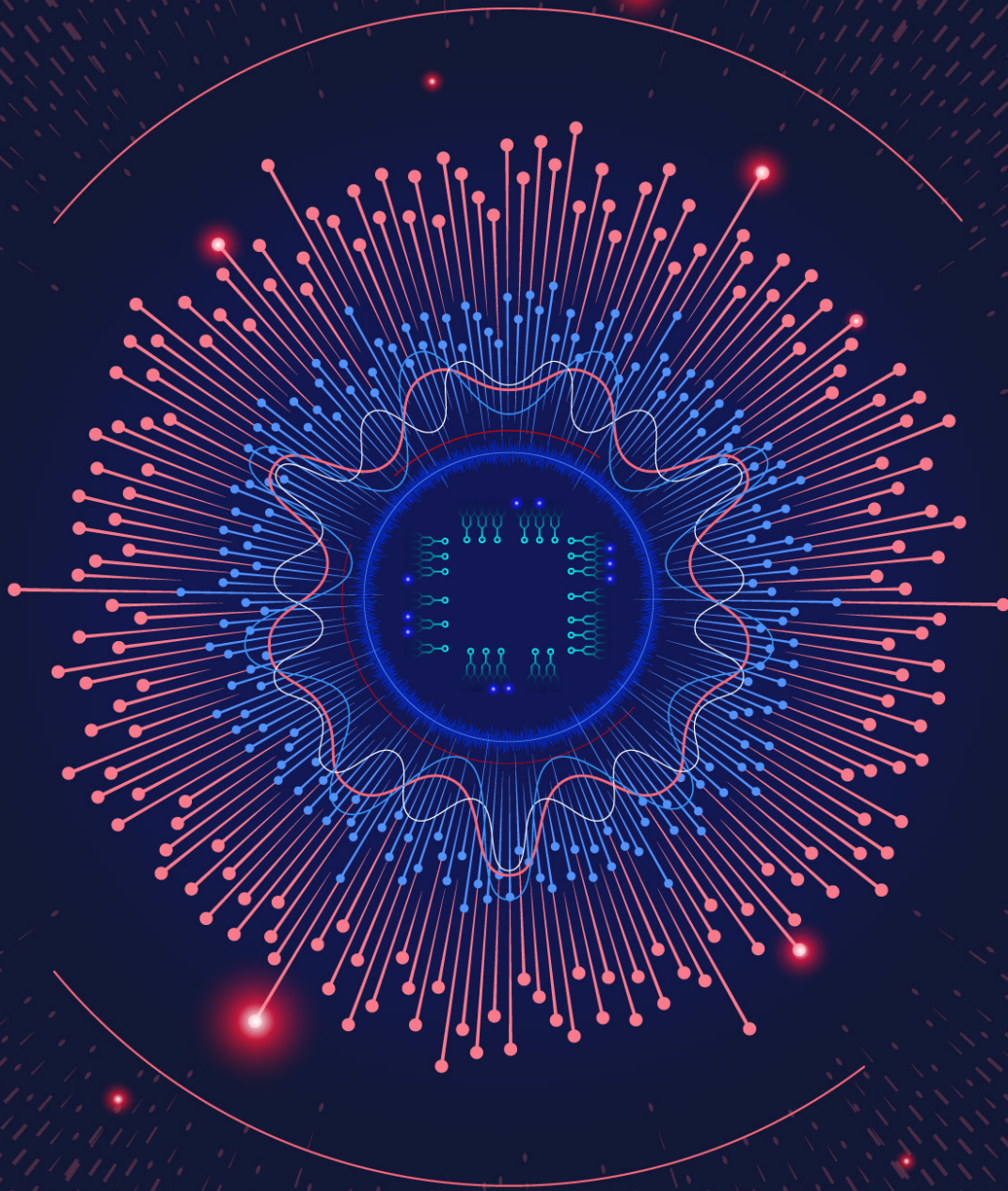


 smarsh®

 1LoD®



# BUY-SIDE SURVEILLANCE LEADERS BRIEFING

JANUARY 2022

# Playing catch-up: the future of buy-side surveillance

Buy-side institutions feel they are under less pressure to re-engineer their surveillance processes – whether from regulators or as a result of alert fatigue – than sell-side firms. But now that hybrid working has become the norm, the buy side is taking another look at communications surveillance, the integration of comms with trade, and thus at newer technologies such as machine learning and artificial intelligence.

*"Hearing insights from peers and innovators at the forefront of our industry at the Buy-Side Surveillance Leaders Briefing 2022 was a pleasure and provided valuable context as to how we are all navigating this journey from an Asset Manager's perspective. The debates were varied and well mediated, drawing out thought provoking discussions from the well-balanced panel of delegates. Having the opportunity to hear from a speaker of Lord Blunkett's calibre in such an intimate setting in the heart of Westminster was a real treat, too. Thank you, 1LoD."*

- ADAM MCNULTY, SENIOR SURVEILLANCE MANAGER, HSBC

## Key takeaways

- 58% said trade surveillance needs additional investment to meet regulatory minimums
- Integrating trade and comms surveillance is still aspirational for many buy-side firms
- Moving to a risk-based approach is desirable but budget-constrained
- Buying third-party solutions is preferred to in-house development
- 40% of attendees said legacy technology and data structures were the biggest impediment to adopting new solutions
- Institutions are getting RFPs and POCs wrong too often
- Increased regulatory attention will force the buy side to up its game

1LoD brought together surveillance and compliance leaders in January from some of the most important buy-side institutions in Europe and the US to discuss the challenges of surveillance in the sector and to share ideas about how best to meet them.

The Rt Hon. the Lord Blunkett of Brightside and Hillsborough, the former UK home secretary, opened the discussions, pointing out that the recent scandal in the UK over Downing Street's lockdown parties showed how even individuals who are subject to heavy surveillance can behave recklessly and flout regulations. He said he doubted the surveillance of normal working channels would pick up significant wrongdoing because bad actors would inevitably use unsupervised means of communication.

He added that a reliance on technology to replace trust, collaboration and an ethical work culture was likely to fail: in his opinion, a culture which encouraged people to call out bad behaviour would outperform any surveillance process, regardless of its technological sophistication.

This, in turn, requires a rethink of some of the most fundamental ways in which financial institutions operate: "Culture is a reflection of the incentives and rewards that are built into the process so that people are clear what it is that's expected of them and the rewards that will come from what is perceived to be doing a thorough, good job."

Of course regulations must be followed, he said, while warning that "if you have systems that are so out of date that they don't take account of major social, economic and technological change, then they'll become meaningless. And once they erode, people treat them with contempt."

"This is made harder because there are no decent tools/dashboards that can give the 1st line help to manage risk or derive value – and so they see KYC as a manual costly admin burden/compliance function, not a risk management benefit," they explained.

"The Buy-Side Surveillance Leaders Briefing provided a fantastic opportunity to engage with industry thought leaders to discuss topical issues relevant to our sector."

TOBI AKINGBOLAGUN, HEAD OF COMPLIANCE SURVEILLANCE, LEGAL & GENERAL INVESTMENT MANAGEMENT

## Investing in trade surveillance

Attendees did not say whether they thought that regulations concerning market abuse, customer harm and systemic stability fell into this category but they did reveal that complying with them was still very much a work in progress. Almost 60% agreed that their trade surveillance operations required additional investment to meet current regulatory minimums; only one fifth said that their firms had an efficient and effective trade surveillance process. [CHART 1]

One explanation for these findings could be the Financial Conduct Authority's shift in emphasis in recent years. As one participant put it: "The heat of the regulatory focus in terms of trade surveillance has passed. Now that may be a controversial thing to say, but I would say that trade surveillance was of greatest importance to the FCA around 5 or 6 years ago."

That tallies with two significant events – the release of the FCA paper 'TR15/1: Asset management firms and the risk of market abuse' and the implementation of Market Abuse Regulation, or MAR, in July 2016. Thereafter, there was relatively little emphasis on the buy side until MiFID II came into effect in January 2018, followed by the Senior Managers and Certification Regime, or SMCR, which was applied to asset managers in the UK from December 2019.

One area where participants said that they definitely feel increased pressure is in their arrangements for ensuring the surveillance of hybrid working. Regulators have slowly ratcheted up their expectations in this field since the start of the pandemic. Now that hybrid working is more established, those expectations are receiving a more formal treatment.

For example, in October 2021 the FCA released an update stating that firms will have to prove that remote working does not or is not likely to cause detriment to consumers, damage the integrity of the market, increase the risk of financial crime and reduce competition. In particular, control functions must be able to carry out their work unaffected, and firms must be able to meet specific regulatory requirements, for example for call recordings, and for order and trade surveillance.

As a result, asset managers have focused on the need to update their trade surveillance technology in terms of coverage and effectiveness. For example, they are moving away from the use of rules-based models for identifying problematic activity to a more risk-based approach. And to do this, they need more data and, in particular, to add communications surveillance data to the trade data.

"To get rid of noise, it's important to define what good looks like. So, we have seen some of our clients enriching their traditional trading surveillance approach by bringing in additional datasets such as communications, and then building what a good behaviour looks like from their existing trading activity. Having identified 'normal', it is a lot easier to be more effective when you are looking for 'anomalies or misconduct type of behaviour'," said Jerome Lambert, business development director - EMEA, financial markets compliance, NICE Actimize.

Chart 1: Do you feel that your firm:

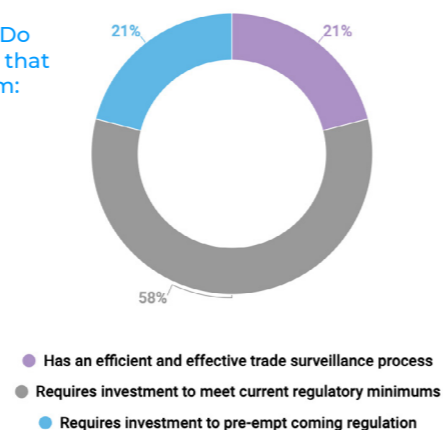
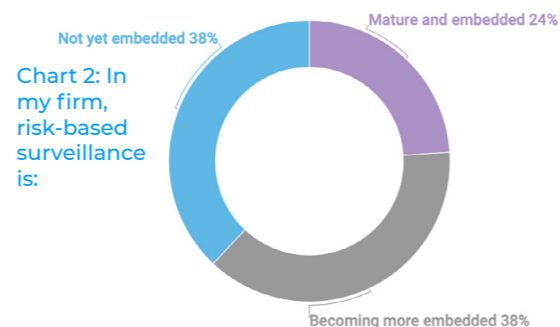


Chart 2: In my firm, risk-based surveillance is:



## The remote comms challenge

This push to integrate comms and trade surveillance and to develop a more risk-based approach was, for most attendees, an aspiration rather than a current programme. Asked about the level of risk-based surveillance in their firms, only 24% said that it was mature and embedded, while 38% said it was not yet embedded. [CHART 2]

A much more pressing matter was the need to ensure regulatory compliance in hybrid work environments, leading the buy side to increase its focus on comms surveillance. As one attendee put it: "When you have to be able to prove that you adequately surveil people who regularly work from home, then having effective email and especially voice surveillance becomes a big part of that."

Vendors also noted the buy side's interest in voice communications. John Holland, senior vice president, Smarsh, said: "If I look back at some of the POCs we were doing three or four years ago, we were regularly finding what I would describe as smoking guns in the e-comms. But now we have seen this change so that the e-comms is relatively clean and the issues have increased substantially in the voice communications. You should, at the very least, bring your voice and e-comms communications and the alerts raised from them together so that you can see the overall picture. The easiest way to do this is to have all your communications be captured into a single repository and then apply the models and lexicons needed to determine whether there is language that should raise an alert being fed to the front end."

The resources devoted to particular voice channels varied widely from institution to institution. For some, the number of recorded lines is limited to small teams of traders and IR professionals. For others, especially those with extensive activities covered by MiFID II, voice is a much bigger challenge. And, as with the sell side, the collision between general data protection regulation (or GDPR), employment law and, in some countries, workers' councils, complicates companies' surveillance efforts. MiFID II compliance generally comes second to data privacy.

That said, it is clear that regulators have increased their focus on voice communication and on the common combined voice and text channels (such as WhatsApp), and that buy-side firms will have to follow the sell side in covering this area.

As Eddie Cogan, partner and head of e-comms surveillance at ACA Group, put it: "Obviously voice has been discussed for some time, but as illustrated in some recent high-profile cases, text channels such as WhatsApp and WeChat have become a very hot topic. With this increased focus, we anticipate that mobile voice calls will soon have increased regulator scrutiny, as they continue to expect firms to raise their game in terms of monitoring their employees working from home."

For most attendees, remote working is now an important part of comms surveillance, which covers the use of new video networking tools such as Zoom, Teams and other channels. Because these channels allow recording, increasingly they have to be recorded. And if they are recorded, then they need to be stored and analysed. Typically, this raises questions about Cloud storage, the sheer volume of video data to be processed and the technical difficulties of extracting the relevant flags from the components of a video (including audio, video, whiteboards, chat, etc.).

The technology to do these things exists today, but there are also legal and compliance decisions that can help to overcome some of the issues. As Rob Houghton, founder, Insightful Technology, explains: "It's actually not difficult to process the video, but you have to decide whether your legal framework allows us to do anything with the video capture to make it more manageable. For example, in Teams, you start with a duplicate copy per speaker. So, are you allowed to take just one copy instead? Am I allowed to change the format of the original data using lossless compression? And so on. If you get legal sign off for that, then video becomes something that actually can be done. And obviously if you don't want to take the video, you can always take the voice out of the video."

This information was taken from the Buy-Side Surveillance Leaders Briefing event in London, 25 January 2022.

For more information on 1LoD please visit: [www.1lod.com](http://www.1lod.com)

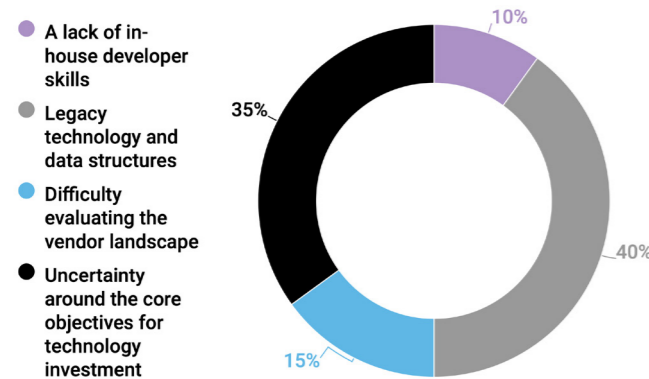
## Getting the right tech

Whether it's analysing video or aggregating the data necessary for more sophisticated surveillance, buy-side organisations need to ensure that they acquire the technology that best suits their requirements and objectives. The vast majority of attendees said that building this technology from scratch was not an option.

However, there were two noticeable exceptions. One very large and specialised firm built its own systems from the ground up, thus avoiding what it saw as the failure of mainstream solutions to solve the key problems of false positives and identifying new forms of market abuse. Another (also very large) firm took the interesting hybrid approach of investing directly in a third-party solution provider, thereby gaining technical expertise and leverage in product development.

Even though buying-in remains the only sensible option, attendees – surprisingly – did not rate vendor evaluation as a significant challenge. Instead, the burden of legacy technology and data structures, and uncertainty around the core objectives for technology investment were seen as the main challenges. [CHART 3]

Chart 3: Is your biggest surveillance technology challenge:



## The devil is in the data

It is no surprise that institutions are struggling with data challenges. These plague all large organisations trying to use new technology to derive insights from their legacy data silos. Attendees complained about the difficulty of getting data from different business lines, the lack of a firm-wide golden source of critical data and the long-standing issues of obtaining, storing and processing data from an increasing number of markets and venues.

Buy-side firms also need to dig deeper into the data that is available to find the more sophisticated types of market abuse being perpetrated today. As Melissa Watras, director of product, Trillium Labs said: "Of course it is important to aggregate and normalise data and create that golden source, but there are also specific data needs people might want to think about. For example, to detect some kinds of misconduct you really need to look at the full order book depth – both level one and level two. So we look to try and create visibility like that as well as in terms of broader data visibility."

*"Good event with engaging speakers. Good to share thoughts and ideas. The meeting provided a good temperature check of our peers and provided reassurance and challenge to our current thinking."*

STUART LIDDLE, HEAD OF FIRST LINE CONTROLS FUNCTION, EMEA., INVESCO

## What are we trying to do?

The problem of identifying objectives feeds through to the entire request for proposal (RFP) and proof of compliance (POC) process. Too often, procurement departments take over the RFP process, asking dozens of unnecessary questions rather than focusing on how the technology will be used to solve real surveillance issues. And POC processes are too different from vendor to vendor; in many cases they are not run on realistic datasets, and do not generate provable results that are measured against specific KPIs. Tech buyers also need to think about longer-term issues around suppliers: their size, their culture and their flexibility.

Relying on smaller fintechs for critical applications is a difficult decision for larger, more conservative organisations, particularly when, as one vendor present said: "I really feel for you; you are taking a leap in the dark and you simply have to trust what people tell you [about their solution]."

But sticking with the industry standard products brings its own risks too, and attendees were split on the pros and cons. The safety of using the same solutions as everyone else appealed to some; but others felt that by engaging with a smaller company, it is possible to partner more effectively with them and come up with solutions to suit requirements in a much more effective and agile way.

Vendors said that flexibility and openness to customisation was critical. As Rob Mason, global regulatory lead at Relativity, pointed out: "You are ultimately buying a service that has to be able to evolve with your needs. But there is a difference between a continual back-and-forth of requests, prototyping and evaluation, and buying a platform that is inherently extensible and flexible by design. Ideally you are looking for a solution that allows you to adjust the product as you change without having to go to the vendor. That is the way I think the market is moving so I think people should definitely probe vendors' mentality towards adaptability."

## No time to lose

These decisions around technology are becoming more urgent. The regulators will no longer tolerate surveillance processes to be compromised by COVID. And enforcement is ramping up. At the end of 2020, for example, we saw the first FCA enforcement action for any of the three substantive offences under MAR (market manipulation, insider dealing, and unlawful disclosure of inside information).

There have been good reasons for the buy side to lag the sell-side in the past. Those reasons will not hold up in the future. It's time to play catch-up.

