REPORT

THE 2024 SURVEILLANCE BENCHMARKING SURVEY & REPORT

Key takeaways

A third of banks will be increasing their surveillance spend in the next 12 months

44% of banks will buy new trade surveillance technology in the next three years

86% of respondents do not use trader profiling to filter alerts and many will not

61% of respondents anticipate using artificial intelligence (AI) -driven risk identification in their trade surveillance function

73% of banks need to upgrade their capabilities or start from scratch in cross-product market abuse

Surveillance technology buying decisions now include Chief Risk Officers, Chief Operating Officers and Heads of Audit

83% of banks are going to buy new e-comms technology in the next three years

74% of banks will buy new voice surveillance technology in the next three years

55% of banks now require model risk management (MRM) approval for surveillance model calibration

91% of respondents anticipate using AI-driven risk identification in their communications surveillance function

35% of banks surveyed will be spending more than US$5 million on change-the-bank (CTB) projects in the next 18 months, with almost a quarter saying that they will spend more than US$10 million

74% of people say that they either already use or are planning to use large language models (LLMs) in their market abuse surveillance functions in the next 12 months

Introduction

These are the results of 1LoD's completely updated version of its 2020 Surveillance Benchmarking Survey & Report. Since then, we have had thousands of conversations with surveillance leaders across the industry, including detailed consultations with the members of our Surveillance Leaders' Network, who represent the most experienced surveillance leaders in the market.

This survey is the result of those conversations and it incorporates a host of new datapoints designed to help you benchmark your own trade, e-comms and voice surveillance processes against your peers.

There are three big picture takeaways from the survey and the interviews that were carried out alongside it:

1

First, the influence of the regulators on how surveillance teams are organised, how big they are, what technology they buy and when, and what areas of surveillance they are focusing on at any particular time is even more pervasive than ever. Banks under enforcement or in some form of remediation will focus in extreme detail on the area of failure and will spend whatever it takes to comply. With remediation completed, spend tails off and the organisation reverts to its original technology timeline.

Last year's WhatsApp fines drove a spike in e-comms spending on messaging and collaboration tool channels. Regulatory statements on culture have broadened surveillance scope and the latest focus on venue completeness is driving venue audits and a host of new workflow and visibility developments between surveillance, the business and venues. And that focus seems to have driven the latest large fine – US$350 million for JPMorgan Chase & Co– which is larger than any of the WhatsApp fines. We can expect banks to switch their focus to venues and feeds into trade surveillance engines even without further enforcements.

2

Second, and related to the first, mid-tier banks can no longer get away with minimalist surveillance. The largest banks have clearly attracted the most regulatory attention thus far, and smaller institutions could be forgiven for thinking that their size and market influence have been deemed below the radar. However, it's becoming clear that regulators are now turning their attention to smaller institutions, and when they do, they can be just as aggressive as they are with the larger firms. In particular, regulators have cottoned onto the fact that smaller banks can still have significant influence in particular assets or markets and that they may not have put in place surveillance tooling proportionate with that influence. Smaller banks cannot argue that they have no impact on market integrity.

3

Third, technology really is now starting to transform the surveillance function. While AI/ machine learning (ML) has had the most high-profile impact on voice and e-comms solutions, and on spending plans in those areas, these technologies will also finally break the logjam in trade surveillance. Here, surveillance professionals have traditionally been pessimistic about their ability to replace legacy systems or even upgrade them to make any significant difference to the problems of false positives. Now, as this survey shows, a majority of banks feel that AI will change the calculus here and they are planning to invest.

As new technology develops, it will have two other key effects: first it will force banks to change their outmoded data practices as these become unsustainable obstacles to modern levels of efficiency and effectiveness. Second, it will highlight a strategic choice that has always existed but rarely been acknowledged: do banks want to be 'high-tech low-people', or 'low-tech high-people'.

PEOPLE

Who, where, how many?

Over the past eight years. 1LoD has hosted many debates on the optimal structure of the surveillance function. In general, banks say that they are indifferent as to whether surveillance is a 1st or 2nd line function, despite the fact that they also believe that market and product expertise is a must, and despite the fact that organisations should be able to derive commercial benefits from close analysis of the behavioural and other data collected by surveillance teams.

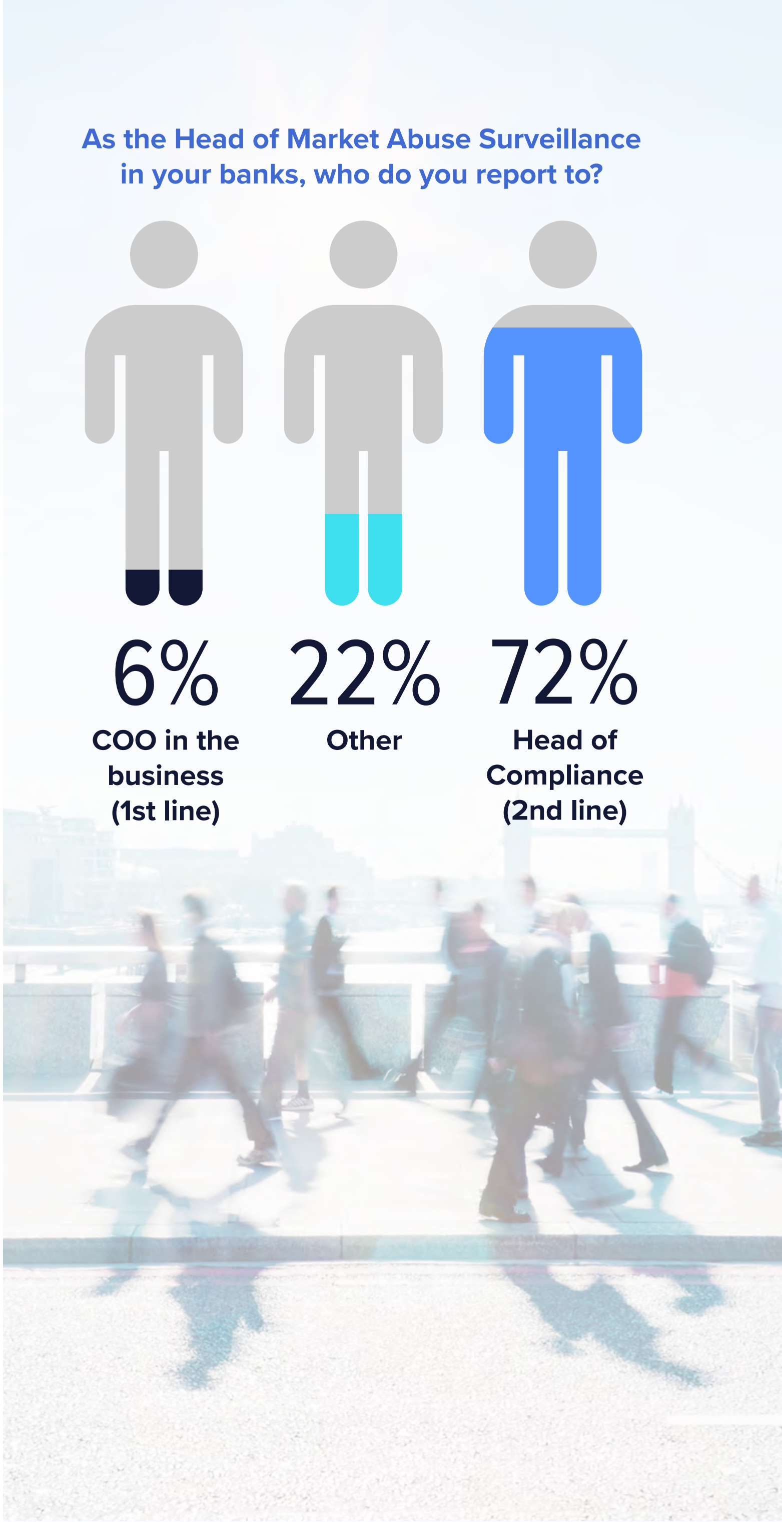
In practice, almost three quarters of those polled reported into the Head of Compliance and just 6% reported into a COO in the 1st line. The rest reported into a mix of compliance assurance or a risk and compliance COO.

Just one reported into the CRO, an interesting outlier that perhaps indicates a future in which the complexities of non-financial risk are understood to be a great deal more material than simply a regulatory issue. CROs are mentioned as key stakeholders in surveillance technology sign-off and procurement and so it may well be the case that in future Senior Risk Officers will play a greater part in fundamental surveillance decisions.

While it may not be surprising that surveillance rolls up to compliance, it raises the questions: is this how it should be? Do banks see surveillance as essentially a matter of limiting regulatory enforcement? To what extent is the business interested in the information generated by surveillance?

Poll respondents asked these questions essentially said the same thing: yes, the business is interested in surveillance, but what they want is reassurance that they are covered from a regulatory standpoint. And yes, most of the nuances that we see in surveillance structures, spend and technology reflect regulatory emphases and enforcements. Banks focus on things the regulators highlight (like cross-market abuse and messaging). They spend most when they are in remediation and they spend more on areas under enforcement than elsewhere. And that spend falls as remediation is completed.

This picture of surveillance as a ship blown unpredictably by the winds of regulation is unlikely to change. Regulators at the latest XLoD Global - London vowed to make non-compliance more expensive than compliance – an acknowledgement that previously banks could risk-accept compliance gaps to their economic advantage. And the latest fines seem to show that they meant it.


As the Head of Market Abuse Surveillance in your banks, who do you report to?

Why so many onshore teams?

In terms of the size of surveillance operations, the average function employed 130 people split 53 EMEA, 46 APAC and 31 Americas. Behind this one average lie four different groups of institutions: the very largest global banks with significant fixed-income, foreign exchange, commodities and equities businesses, the second-tier regionals again with operations in those asset classes, smaller local banks or larger regionals active in fewer market segments, and then smaller institutions of various kinds.

The basic geographical split may seem unsurprising, with surveillance staff located where banks' most significant operations were and also in those locations where regulators have been most assertive in looking at market abuse and conduct issues.

However, it means that more than half of all surveillance staff are located in onshore hubs – the most expensive place to put them, with another 16% near-shore and almost a third offshore. This seems odd given that, on average, 81% of those staff are looking at alerts (which also explains the 92% of staff who are VP or below). Why put so many people doing this in expensive places?

It turns out that there are several different reasons. The first is maturity. Even very large banks sometimes started with what some call the subject matter expert (SME) strategy: when establishing a strong surveillance foundation, some institutions deliberately centralised teams in the core business locations to exploit subject matter expertise. Only when they are satisfied that the surveillance process is right are they then confident enough to start offshoring. Two of the world's largest banks are still only now building out a level one (L1) analysis capability in India for this reason.

Others explain this reliance on expensive locations for staff by saying, "Very few of the locations in which people near-shore or offshore are really low cost anymore, so it may be that the difference between hub and those locations is not that great."

And there is also a difference based on team size. While larger banks with large teams of L1 analysts will usually have them offshore in India, Poland or Portugal (the most frequently mentioned locations), the mid-sized and smaller players have often made a conscious decision to have everyone onshore for reasons of visibility and quality control. They also have smaller alert pools to analyse and so can run a larger percentage of them through more senior teams of the kind that are generally kept onshore by all the banks.

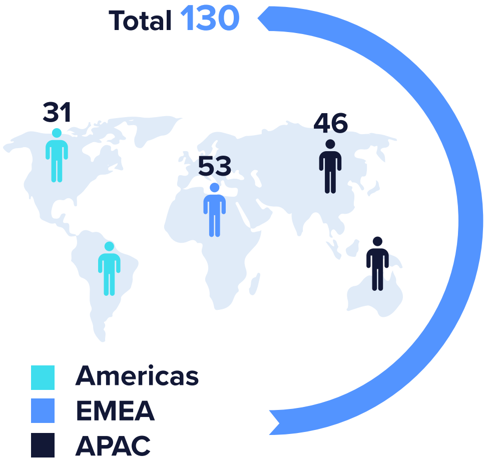
Banks also talk of an upper limit to offshoring – around the 50% mark. "You should only ever offshore about 50% of your function, because the offshore team can't do the escalation, or the risk assessment and they certainly can't do the development, and all of the other infrastructural work that is involved in surveillance. While on the other side, you can make a conscious decision to not offshore and to use fewer people who are more senior and can process alerts from initial query through to close more efficiently. But to make that work, you've got to invest in your technology because you don't want expensive people in the hub going through thousands of wash alerts."

Onshore? Watch your back

That said, even banks who deliberately started with the SME in-hub model are looking to change. One participant explained, "My message to my [L2] teams is 'you need to be looking at everything you do and you need to be figuring out what could be outsourced or given to your colleagues. We are definitely heading in the direction of saying, 'if you can't justify your added value to the business, then why are you here? Why wouldn't somebody look at you and ask why can't we do that out of India?'"

As for that very high percentage of staff (81%) performing alert reviews on a daily basis, the range is fairly narrow regardless of institution size. Some banks have got the ratio down to around 60%, others are closer to 100%. To an extent, there may be other drivers embedded in the numbers too.

How many people work in your surveillance function by region (including offshore resources)?



How many full-time equivalent (FTE) headcount in your team are performing alert reviews on a daily basis?

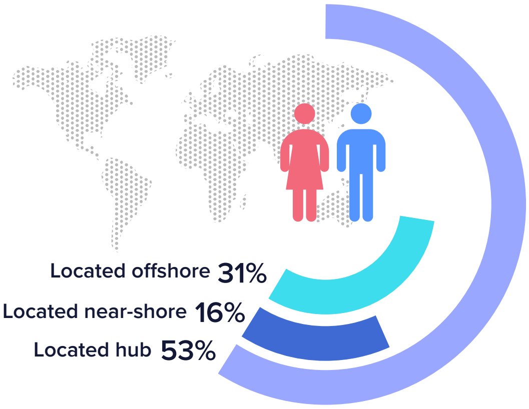
Average 103

Firms with more mature functions might be expected to have added additional support systems (e.g., around technology and data) that would reduce the percentage of people trawling through alerts.

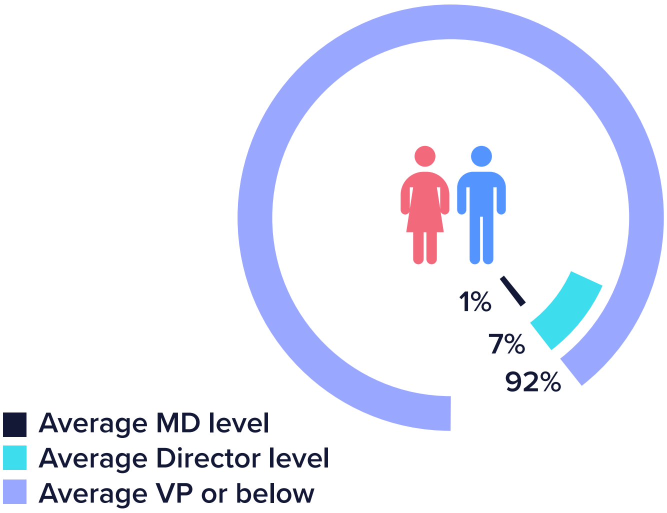
On the other hand, institutions that have not been sanctioned for surveillance failures may feel more comfortable with having fewer of those support functions around them – which would, all other things being equal, drive the percentage of staff looking at alerts up.

More than half of all surveillance staff are located in onshore hubs – the most expensive place to put them, with another 16% near-shore and almost a third offshore. This seems odd given that, on average, 81% of those staff are looking at alerts (which also explains the 92% of staff who are VP or below). Why put so many people doing this in expensive places?

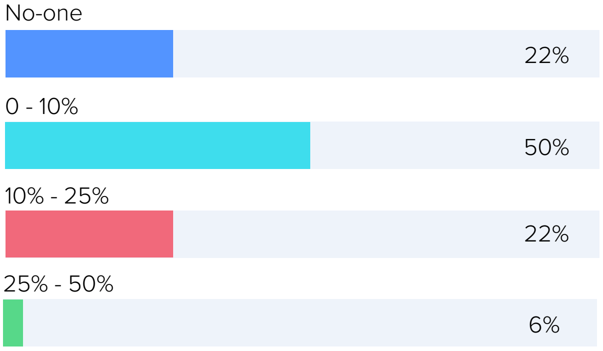
What percentage of your surveillance function headcount is currently located in:



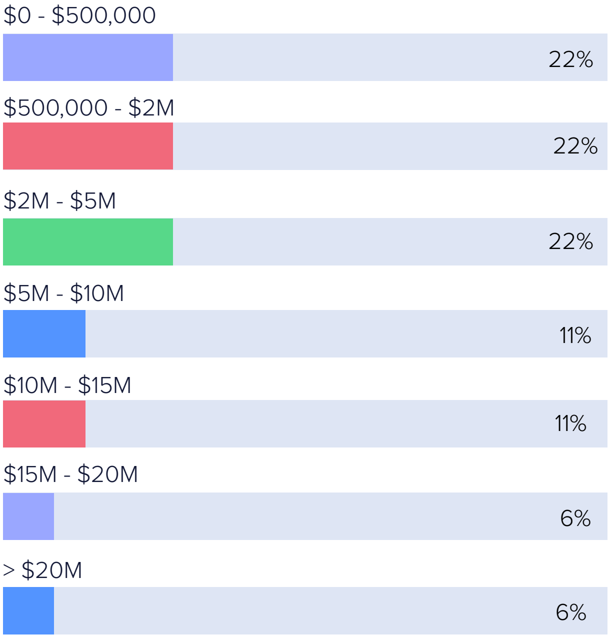
How many of your surveillance function headcount are:



What percentage of employees in your surveillance function are working exclusively on CTB projects?



What is your planned investment spend (US$) in CTB surveillance projects over the next 12-18 months?



Investing in change

That percentage of staff focusing on alert reviews shows that just keeping on top of Business as Usual (BAU) is a full-time job for many surveillance teams. Yet the pace of change in data science, in cloud computing and in advanced textual and statistical analysis means that banks must also devote time and resources to planning for and building the next generation of surveillance.

Reflecting on this, 35% of banks surveyed will be spending more than US$5 million on CTB projects in the next 18 months with almost a quarter saying that they will spend more than US$10 million. These are very significant numbers when totalled across the industry.

However, this is very much a story of haves and have-nots. In the have-nots, half of all respondents said that they had less than 10% of staff on this kind of work and two-thirds were planning to spend less than US$2 million in the next 18 months.

What this means in practice is that these surveillance teams are running these kinds of activities on the side of the desk. Respondents say that this is to be expected for a number of different reasons.

First, budgets. The have-nots all agreed that CTB activities do deserve more dedicated resources. However, they say that given the constraints of the current budget cycle, it's unsurprising that spending is focused on more bread-and-butter surveillance upgrades.

Second, as one respondent said, "It's really hard in the surveillance function to have people only dedicated to change because of the skillsets required. You tend to find that people have particular skills – if you have a fixed-income specialist then they are going to be the escalation point for fixed-income alerts, and they're also going to be the one providing the input into how to design models for fixed-income as well, so they don't have the time or skills to be thinking more broadly about change. You need Project Managers and Data Specialists and so on."

COVERAGE

What are you looking at?

Ensuring regulatory compliance means, first, make sure everyone and everything that must be surveilled is surveilled. After a decade or more of developing conduct and market abuse surveillance, it might be assumed that banks had coverage done and dusted but, as the recent US$350 million fine for JPMorgan shows, a combination of market evolution, regulatory development, budget constraints and technology change creates an ever-shifting coverage landscape in which gaps are constantly appearing.

As markets have changed, the number of venues and communications channels on venues and platforms has exploded. Without a robust venue and connectivity audit process, and without creating a formal responsibility in the 1st line for identifying all venues to surveillance, entire datasets will be missed.

Regulatory change, or simply a change in emphasis, can reveal coverage problems. The recent focus on cross-market surveillance has highlighted how difficult it is to get the quote and order data from over-the-counter (OTC) markets needed to run this kind of surveillance effectively. Regulators' focus on messaging channels led to the discovery of the gaps in WhatsApp's data retention. And regulatory questions around web-based venues have led to a wider look at whether banks are actually capturing and surveilling all of the venues on which they now trade.

Technology change, both internal and external, can create coverage gaps as new data feeds are either missed completely or existing feeds are reconfigured by venues without informing banks. In the JPMorgan case, it seems that one venue is the main source of the issue though it is not clear how the problem arose or was identified.

"The firm self-identified that certain trading and order data through the CIB was not feeding into its trade surveillance platforms," JPMorgan said publicly, referring to its commercial and investment bank. "The firm does not expect any disruption of service to clients as a result of these resolutions."

And budget constraints have led some banks to revisit their surveilled populations in an attempt to focus only on those absolutely required by the regulators. This is not just about money. Surveilling peripheral populations for market abuse risks generate even more of the false positives that plague the surveillance function.

What business lines are you surveilling?

Markets	Banking	Custody	Wealth	Corporate	Retail
100%	77%	23%	36%	55%	14%

Different approaches to scope

The survey reveals that the average population being surveilled is 11,840 (remember that the average team is 130 and spends 81% of its time reviewing alerts). Again, because of the spread of institutions surveyed, that average hides some big differences. The institutions surveyed here fell into four broad categories: smaller institutions, or alternatively larger institutions with very specific business models, with surveilled populations of under 1,000; mid-sized banks with between 1,000 and 3,000 people under market abuse surveillance; bigger regional players with between 7,000 and 15,000 under surveillance; and then the large, global institutions with typically between 40,000 and 60,000 people being surveilled.

Unsurprisingly, everyone responding to our survey runs surveillance across their markets business. But more than three-quarters also surveil in banking, a third surveil their wealth business and a quarter surveil their custody activities – with a lower percentage for retail.

One driver of the surveillance of non-markets activity is simply that because all trades are ultimately booked via systems and individuals who are surveilled, regardless of which business originated them, then there is a sense that those other businesses are surveilled by default.

However, there is also plenty of broader communications surveillance, and the more mature the surveillance programme, the more is brought into scope. “We can’t rely upon detecting everything in trade,” says one participant. “So, we absolutely look at anyone in any department who has access to material non-public information (MNPI) or who has the ability to fall foul of the market abuse and misconduct regulations.”

In practice, mature banks tend to roll everyone in corporate and investment banking into e-comms surveillance regardless of explicit regulatory prescription. Increasingly, this even includes compliance and surveillance itself. However, this does not yet extend to voice. Where there is no regulatory requirement for voice surveillance, it is rarely employed.

Only the very largest institutions say that they surveil their retail businesses using market abuse regulation (MAR) surveillance infrastructure. Here they are looking for very specific behaviours that might indicate that a retail client is part of a broader attempt to commit market abuse, rather than simply trying to identify unusual transactions. Since the transaction sizes in those specific instances far exceed retail norms, alerts are extremely rare.

Regulatory pressure will drive more surveillance of non- markets businesses in future. For example, as certain markets have developed – for example, the syndicated loan markets – the potential for abuse has arisen even where, strictly speaking, it could be argued that the products do not fall under MAR.

Keeping communications coverage under control

The biggest fundamental issue in communications surveillance is the burden of increased coverage. It's been clear for some time that most banks have chosen to surveil a significant number of both voice and e-comms channels in the absence of an explicit regulatory requirement (as distinct from the need to capture for record-keeping purposes).

There are many reasons for this but clearly two significant drivers are a need to surface market abuse risk that is missed by or hard to detect in trade surveillance, and a desire to detect broader conduct and culture risks.

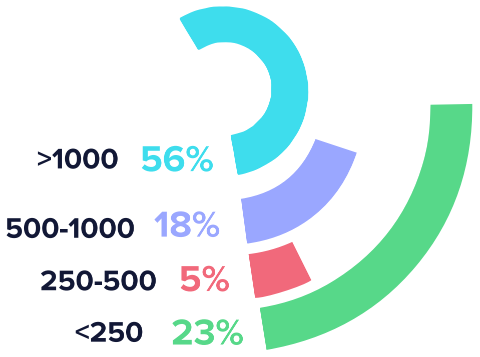
The question banks face in having done this is to what extent they feel it necessary to continue to add channels to their surveillance efforts as regulators focus on new channels, missing venues, and the communications channels embedded in new venues and applications – all of which are evolving all the time.

The latest focus on, and fines around venues, has initially created enforcement around capturing trade data for surveillance but it has highlighted just how many venues have embedded communications capabilities, and how these can fly under the radar of record-keeping and surveillance teams. It also exposes the gaps between vendors, the business, surveillance and compliance in tracking these channels.

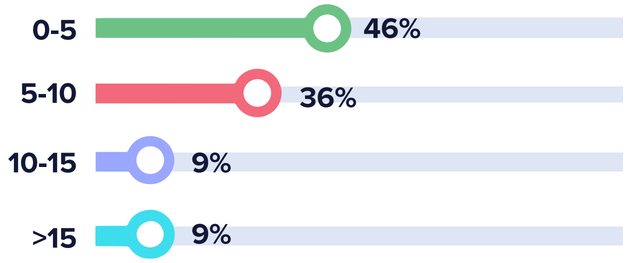
So, just as with WhatsApp, banks have to decide at what point they collect those new and multiplying datasets for record-keeping purposes, or not, and if they do collect them, then which do they leave unsurveilled to keep coverage (and alert volumes) manageable.

Banks responding to this survey all agreed that they will increasingly have to take a risk-based approach to these new channels. Where a channel is public or multilateral, like a chat room or social media space, the assumption will probably be that no-one would post misconduct-related information there. Where a channel is private and bilateral, then it is more likely to be captured and surveilled. If a channel does not have a free text capability, it is less useful as a way to communicate. Banks will increasingly have to make risk-based decisions around these kinds of variables to avoid having to capture and surveil everything.

How many lexicons are you using?



How many languages does your communications surveillance function cover?



Getting language right

In terms of language coverage, almost half the banks polled surveilled between zero and five languages. This may seem too small a number, but if you exclude Chinese and Indian languages and dialects, and focus on the languages spoken in the most heavily traded markets globally, then a list that includes English, French, Spanish, German and Portuguese, for example, would give a lot of coverage in Europe and Latin America. Banks regionally focused in Asia or the Middle East would have to substitute in Korean, Japanese, Arabic and, potentially other languages. But five would cover a lot of ground.

For larger institutions, 36% of banks have coverage in up to 10 languages – realistically giving them coverage of all the most significant markets where market abuse is a regulatory concern.

The real question is how much of the comms in these languages is surveilled and how accurate is the output? When asked these questions, most banks admit that they still use random sampling for much of this monitoring, and they also admit that the alerts are overwhelmingly false positives.

This is an area of surveillance where new technology is probably having the biggest impact. First, it is rapidly removing the 'how many languages' problem. Cheap AI-driven voice transcription and translation is a reality and there should soon be no reason, except cost, to exclude a significant language from surveillance.

Second, ML- or AI-driven tools are also transforming the analysis of these transcripts away from high false-positive keyword searching to smarter natural language processing (NLP) analysis that can not only distinguish between innocent and not-so-innocent uses of the same words and phrases, but can also flag bad intentions and other forms of problematic behaviour.

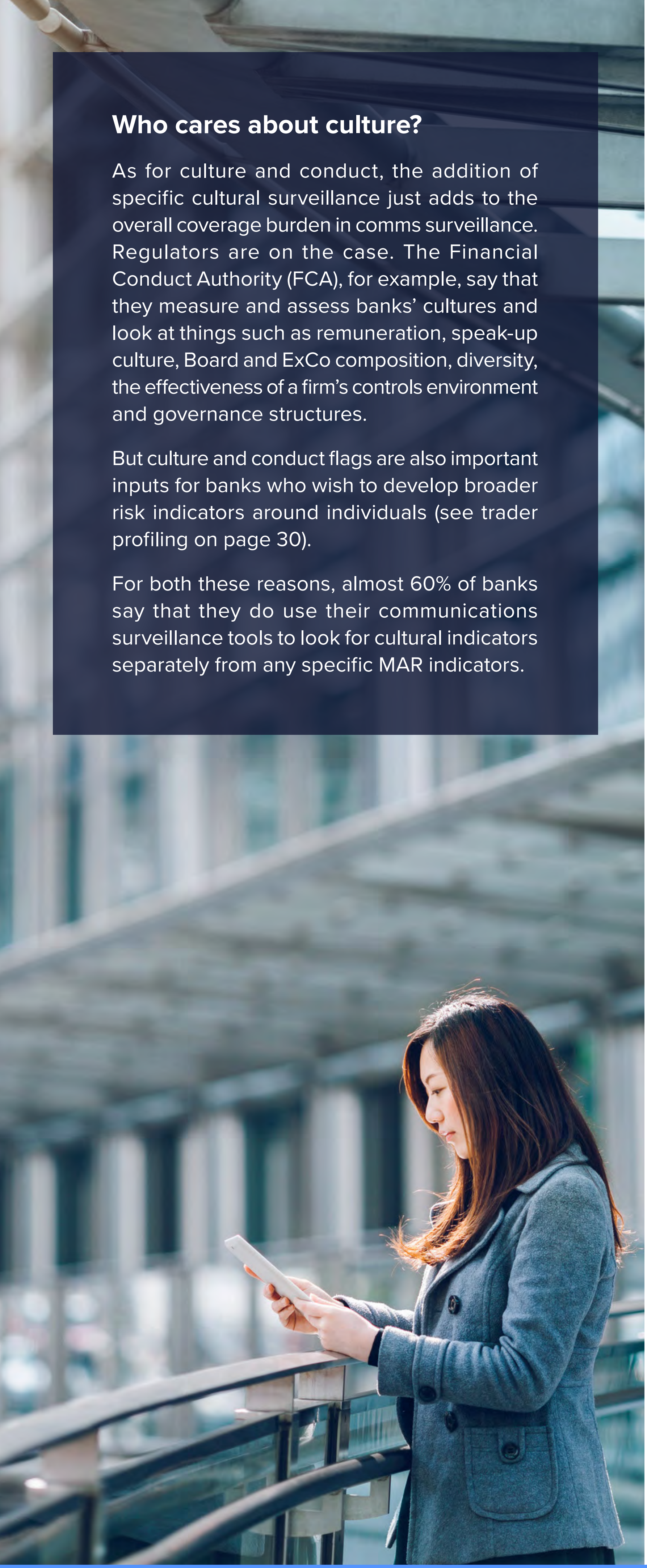
Third, these tools automate the core analysis and so eliminate the need for sample-based surveillance, allowing banks to be sure that they can monitor all their voice and e-comms channels in full.

Despite the use of NLP, banks still rely heavily on lexicons. In general, a lexicon is a set of words or phrases tied to a specific scenario or model that is mapped to a particular behaviour prescribed by regulation. Sometimes each lexicon represents one of several scenarios that fall within that behaviour. Each lexicon, especially if it is being used within an NLP model, can contain thousands of words or phrases.

When asked how many lexicons they are using, banks' responses ranged from under 250 to more than 1,000. The larger numbers may seem high, and some respondents were surprised by the cost implications. But it is clear that some respondents were referring to much smaller word lists for specific searches or even, in some cases, individual phrases.

The key finding here is that no-one said zero. In other words, lexicons remain an absolute mainstay of communications surveillance despite the overwhelming preference shown for investment in new, AI/ML-driven technologies. The sheer number of lexicons used is probably a sign of the inefficiency of legacy systems and represents costs that can be taken out of the process at some point.

The real question is how much of the comms in these languages are surveilled and how accurate is the output? When asked these questions, most banks admit that they still use random sampling for much of this monitoring, and they also admit that the alerts are overwhelmingly false positives.



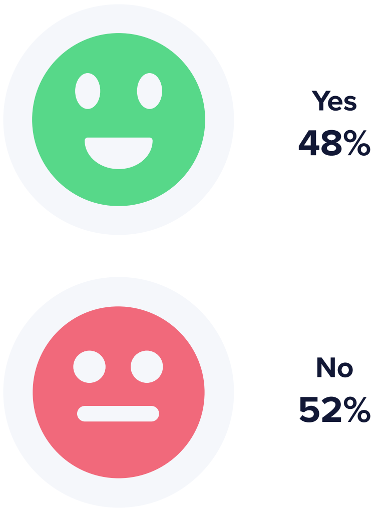
Who cares about culture?

As for culture and conduct, the addition of specific cultural surveillance just adds to the overall coverage burden in comms surveillance. Regulators are on the case. The Financial Conduct Authority (FCA), for example, say that they measure and assess banks' cultures and look at things such as remuneration, speak-up culture, Board and ExCo composition, diversity, the effectiveness of a firm's controls environment and governance structures.

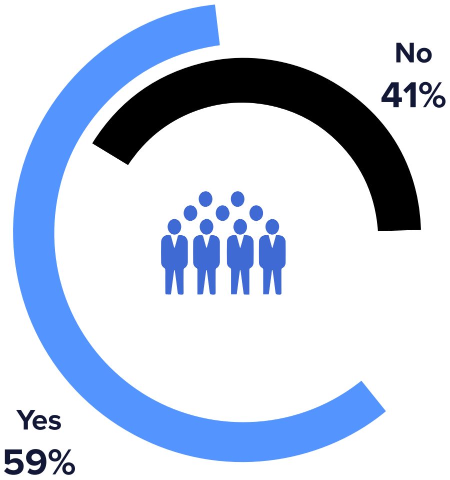
But culture and conduct flags are also important inputs for banks who wish to develop broader risk indicators around individuals (see trader profiling on page 30).

For both these reasons, almost 60% of banks say that they do use their communications surveillance tools to look for cultural indicators separately from any specific MAR indicators.

Is there a concern about the use of emojis?



Are you using your communications surveillance tools to proactively monitor culture? That is, not if it is discovered when surveilling for MAR but looking for cultural indicators separately to MAR?



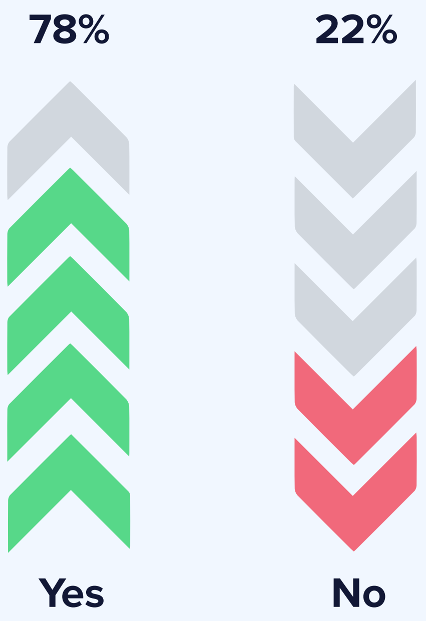
Surveillance budgets rising

As the most recent fines have demonstrated, surveillance is never 'done'. Even for those not under some form of regulatory process, coverage gaps must be plugged and effectiveness improved.

Interestingly though, more than three-quarters of respondents believe that they have sufficient budget to build and maintain their surveillance functions and effectively manage market abuse risk. This is interesting for two reasons: first, it's just unusual for department heads to express satisfaction with their budgets ever!

And second, with an increasing regulatory burden, significant coverage holes evident in industry-wide practices and the need to invest in new technology, one would expect budgets to be struggling to keep up in a cost-constrained environment. So, the implications here are that budgets are rising at last.

Do you have sufficient budget to build and maintain a surveillance function capable of effectively managing the risk of market abuse within your bank?



One interpretation of this result, backed up by conversations with respondents, is that many people interpreted the question to mean 'do you have enough budget to cope with planned BAU?'. The answer to this is 'yes'. However, they cautioned that this does not mean that they believe that budgets are necessarily sufficient to cope with the additional demands that are likely to materialise.

> Interestingly though, more than three-quarters of respondents believe that they have sufficient budget to build and maintain their surveillance functions and effectively manage market abuse risk.

To that point, another reason at least some people are satisfied with their budgets is because they are in fact rising.

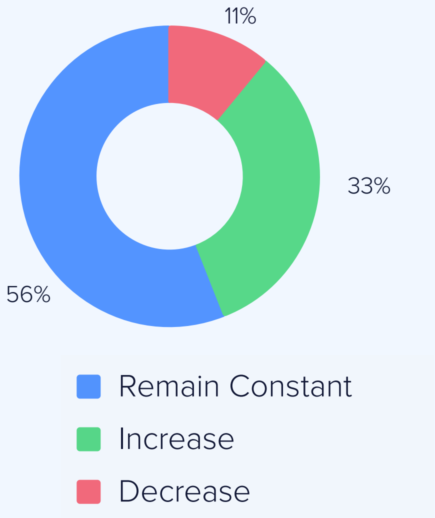
While many institutions will have to do more with unchanged budget and headcounts, a significant number expect bigger budgets and more people. A third of respondents expect increased surveillance budgets for the next year and almost a quarter expect to be hiring more people.

A closer look at the responses reveals that budgets closely track two things: maturity journey and regulatory enforcement.

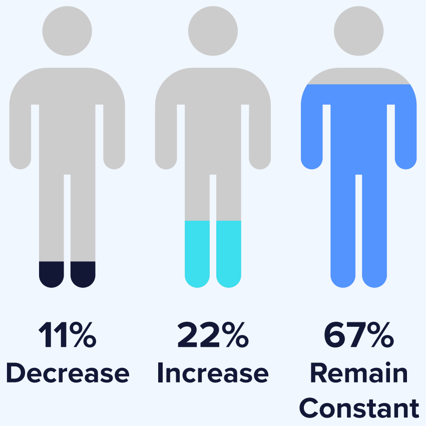
Coverage

The increased spend is largely concentrated in middle-tier banks still working hard to bring their surveillance operations in line with regulatory expectations. But there is also a correlation between remediation programmes and budgets. Unsurprisingly, when regulators demand a particular outcome, money is invested to achieve it and budgets re-normalise afterwards.

How effective do you feel existing controls are to detecting failures?



How do you anticipate the headcount in your surveillance function changing over the next 12 months?



A small number of very large institutions expect both budget and headcount to fall. Again, this reflects their maturity journey: after years of investment, particularly in better data structures and newer technology, these institutions are finally seeing a payoff in terms of efficiency. It may be controversial to say it publicly, but one of the reasons for technology investment is to reduce headcount and so cost base. These banks are seeing the first fruits of that investment.

Looking at where spending increases will be targeted reveals that e-comms and voice surveillance, not trade, are the main recipients. At first glance, this may seem odd. After all, survey respondents were unanimous in their opinion that trade surveillance was the foundation of their market abuse programme and that it was "by a long way, the bigger risk".

By this they simply mean that detecting the key abusive behaviours defined by regulation depends on trade surveillance: it's still hard to find anyone to say that voice or e-comms surveillance are primary mechanisms for detecting market abuse.

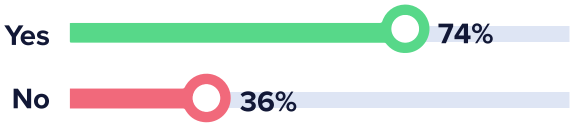
There are two big picture drivers of the interest in voice and e-comms spending.

First, regulatory enforcement: the WhatsApp fines are the most obvious example of a regulatory driver for spending on comms, and the effect of those fines is still being felt in e-comms surveillance programmes.

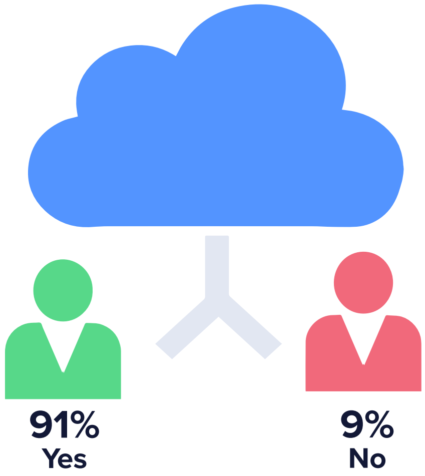
Second, in communications, new technology is becoming available that holds out the promise of big increases in efficiency and effectiveness – with AI/ ML a part of this. The same is not perceived to be true to the same extent in trade surveillance, where the established systems maintain their grip on the marketplace and where technology – at least 3rd-party technology – is not seen as an easy answer. Venue completeness and data availability are still viewed as the key challenges.

TECHNOLOGY

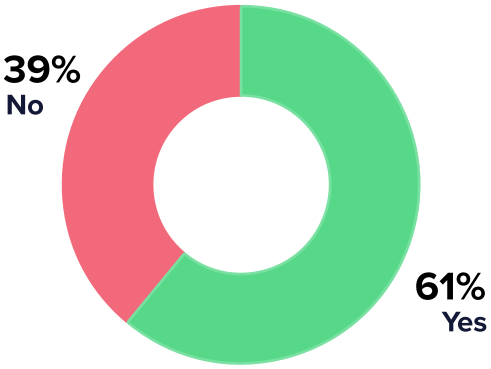
Are you using or planning to use LLMs in your market abuse surveillance functions in the next 12 months?



Do you anticipate moving your technical architecture from on-premises to the cloud in the next 24 months?



Do you anticipate leveraging AI-driven risk identification in your trade surveillance function?



Is AI the surveillance gamechanger?

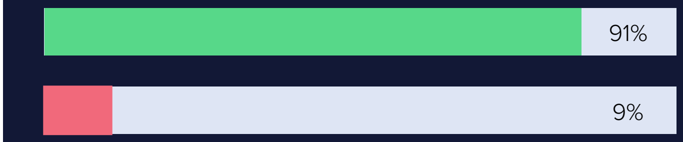
Potentially the biggest gamechanger in market abuse surveillance is technology. AI is the current hot topic across trade, communications and more prosaic workflow functions, with 74% of people saying that they either already use or are planning to use LLMs in their market abuse surveillance functions in the next 12 months.

The range of use cases is surprisingly broad but the more direct use cases for AI/ML extend beyond LLMs, and are already providing much enhanced translation and transcription of voice data, as well as NLP-driven deep analysis of text-based communications. As the banks' investment plans show, it is in both voice and e-comms that institutions can see big gains in effectiveness and efficiency. And to back that up, 91% of respondents anticipate using AI-driven risk identification in their communications surveillance function.

Perhaps more interestingly, even in trade surveillance, where banks are more sceptical of the scope for transformation of an inefficient and ineffective function, 61% of respondents say the same.

Here the hope is that network and behavioural analytics will allow surveillance teams to detect previously hidden patterns in trade and other data, with a combination of pre-alert and post-alert applications.

Do you anticipate leveraging AI-driven risk identification in your communication surveillance function?



Trade surveillance: banks' tech needs unfulfilled

This AI-influenced optimism about the future of trade surveillance is not universal. Most banks agree that while trade surveillance is the bedrock of their surveillance operations, innovations have tended to focus on voice and e-comms. This leaves trade being done, as one respondent said, "much as we did it 10 years ago, which is with systems and models designed for the listed equity markets and for a much lower volatility environment. We are now in a very different world."

That world includes vast numbers of alerts, most of which are false positives because models designed for low volatility struggle as volatilities rise; it includes commodities and fixed-income; and it includes an increasing data availability and ingestion problem.

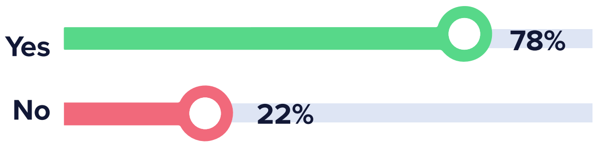
The latest fines around missing feeds are larger than any WhatsApp-related enforcement, and getting data from venues, assuming surveillance has an up-to-date record of all those being used, is hard. Firms are also moving towards a view that they do not need just the trades and orders, but all the quote data too.

"With comms, we have the data – that is the simple bit. What you then do with it is not so simple. But we have it. With trade, the data is the biggest challenge. I'm starting to think that trade and order data, and especially quotes, are the hardest things to find in a bank, and that surveillance are the only people interested in them," said one participant. "We're still struggling to get the key pre-trade data into our surveillance systems and given how long ago MarketWatch 68 was, that's probably a surprise, but it's also kind of not a surprise, right?"

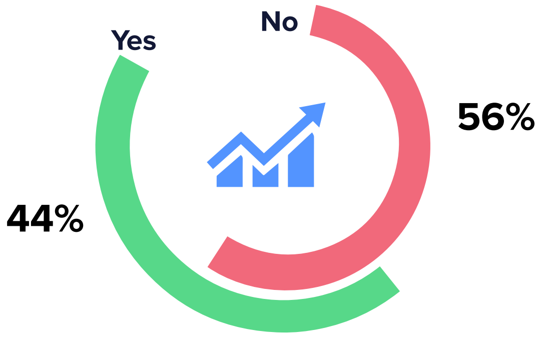
But even if they do manage to get the data, they then face issues with technology. Not only are the legacy systems designed for a different era, some of the new data required causes further problems. As one surveillance lead explained, "When you start putting quotes in, immediately you can discount a lot of the tech out there. And even when the tech can handle it, you just blow the systems out in terms of the message rates."

So, banks can see that their current trade surveillance solutions have not adapted well to the current environment. 57% are either dissatisfied or only partially satisfied with their existing technology.

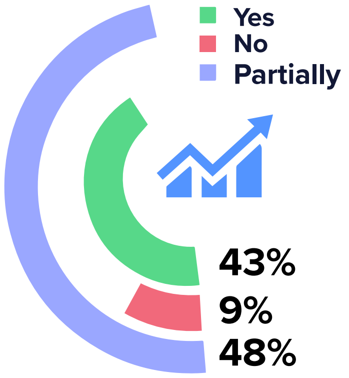
Does your surveillance function have dedicated testing and / or quality assurance (QA) resources?



Does your surveillance function have dedicated testing and / or quality assurance (QA) resources?



Are you satisfied with your current trade surveillance solutions?



They know that some of the fault lies with them and their ability to provide the right data. They know that they are running transformation off the side of the desk, limiting their scope for the kind of root and branch overhaul that trade may need.

But they also perceive there to be a lack of things to buy. More than half the banks in the survey do not anticipate buying technologies to support their trade surveillance capabilities in the next three years – though 44% do.

The other reason banks may be prioritising spend in other areas is regulatory. “What you’re looking at is the power of enforcement, right?”, says one participant. “It’s not just WhatsApp, there is a regulatory focus on communications at the moment and although I may think we need to be spending more on trade right now, the resources will go to where the fines are.”

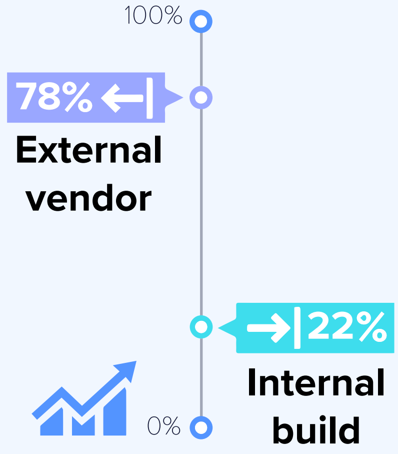
Trade goes in-house

So, what are banks doing in trade surveillance instead of buying 3rd-party upgrades? Well, almost a quarter of them rely on in-house builds and development. This contrasts sharply with voice and e-comms and in some banks – widely separated in terms of size and sophistication – the entire trade surveillance platform is built in-house.

One participant who has gone 100% in-house explained, “We did a vendor proof of concept (POC) versus our existing tooling and the outputs that we saw weren’t sufficiently compelling to suggest that our existing tooling was missing any material gaps in activity. It was debated long and hard and very much still remains something that we would consider at a point in the future, depending on the direction of travel for the business. But we now have a much better handle on what the run costs are for in-house versus 3rd-party and we know how difficult it is and how much it costs to implement change.”

And participants also point out that not everything is about shiny new technology models. Said one, “70% of your problems occur before the alert is generated – so that’s where we should be spending the money not just adding more and more analysts in the near-shore location to deal with the increasing number of alerts as we grow. But the tendency at a lot of banks is often to say, ‘adding cheap staff is a lot easier than investing in technology’.”

What technology supports your trade surveillance?



E-comms surveillance: making comms manageable

"I sometimes think comms is a never-ending investment stream but we haven't yet necessarily got a lot out of that investment as an industry," says one participant. "I mean, how much have we really found? I'm hoping that this investment cycle will yield more."

This participant is one of the 13% of banks not satisfied with their current e-comms surveillance solutions. An additional 52% are only partially satisfied.

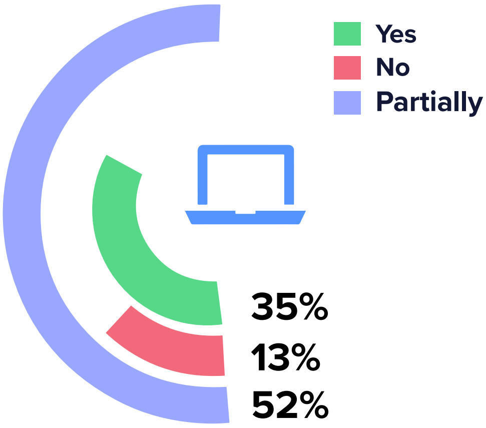
However, versus 44% in trade surveillance, 83% of banks are going to buy e-comms technology and just 9% will use any kind of internal build. This is a demonstration of the optimism with which surveillance professionals view new technologies since 91% currently use external vendors (with whom by definition they are at least somewhat dissatisfied) and will do so again.

As we've seen, the most likely target for this investment will be the next generation of AI-driven translation, transcription and analytics solutions that will, hopefully, give that disillusioned surveillance chief the 'more' that they want from 'this investment cycle.'

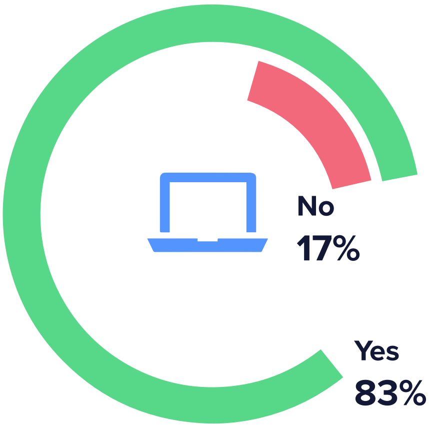
However, it isn't simply about improved functionality. Banks, in private at least, accept that efficiency in reducing false positives, or in giving L1 Analysts better tools to process alerts without escalation, means fewer analysts are needed across the board.

If this new technology works, it will reduce the alert firehose, meaning fewer L1 Analysts; it will deliver sophisticated, smart analytics to guide those L1 Analysts and make their workflows faster – which will again reduce the need for so many of them but it will also move work from L2 to L1 Analysts. Headcount reduction and more offshoring are the goals here, whether vendors and banks are prepared to say so in public or not.

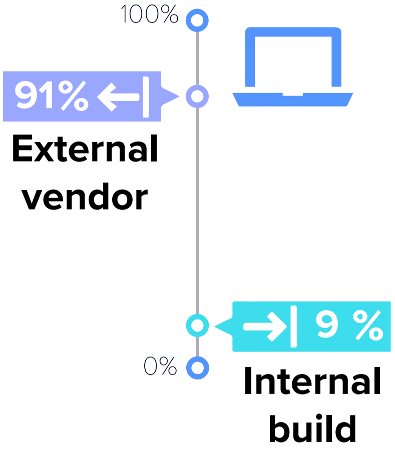
Are you satisfied with your current e-comms surveillance solutions?



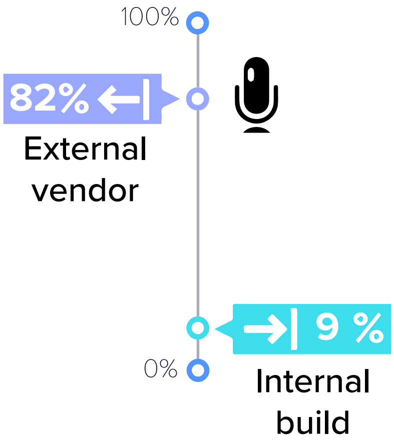
Do you anticipate buying technologies to support your e-comms surveillance in the next 3 years?



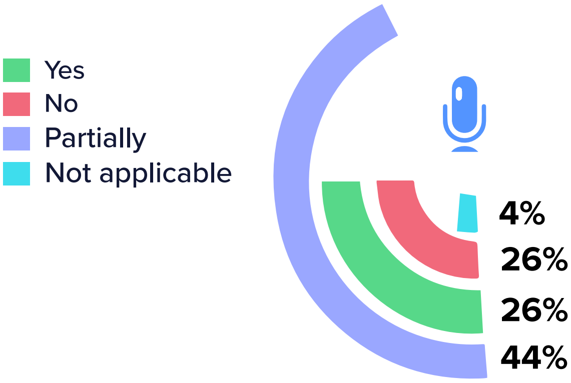
What technology supports your e-comms surveillance?



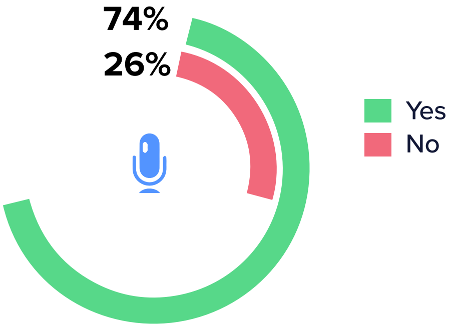
What technology supports your voice surveillance?



Are you satisfied with your current voice surveillance solutions?



Do you anticipate buying technologies to support your voice surveillance in the next 3 years?



Voice: the biggest bang for your buck?

The most outright dissatisfaction with current tooling is in voice surveillance solutions. More than a quarter of respondents are not satisfied with their current voice solutions, and a further 44% are only partially satisfied. Given that 82% use an external vendor, again the fact that 74% anticipate buying new voice technology from 3rd parties illustrates the faith being placed in AI.

There is good reason for that. The most obvious and proven advances made by AI are in the field of language analysis and there are now well-established market leaders in certain aspects of voice communications surveillance and its sub-functions.

The most interesting thing about this anticipated wave of spending on voice is that it is not primarily driven by regulatory pressure or enforcement. There is still very limited need to surveil for voice and there have been no enforcements in this space comparable to the WhatsApp or JPMorgan venue/trade fines. The main drivers are efficiency and the fact that the huge gaps that currently exist in voice surveillance are now not justifiable.

Those gaps, around language and the percentage of communications actively surveilled, were defensible when translation and transcription technology was primitive, and processing and storage were expensive. None of that is now true and it is therefore much harder to explain to a regulator why you only surveil three languages in voice when you do business in 20.

Improving workflow and case management processes

Surprisingly, given the problems that surveillance professionals describe in BAU, more than half the respondents were satisfied with their case management and workflow tools and just 4% were not. One reason for that may be that 26% have built their own and another 35% have created hybrid (built/bought) versions tailored to their own specific needs.

However, banks do believe that AI will make these tools better and create efficiencies across a broad range of functions not uniquely tied in to market abuse surveillance.

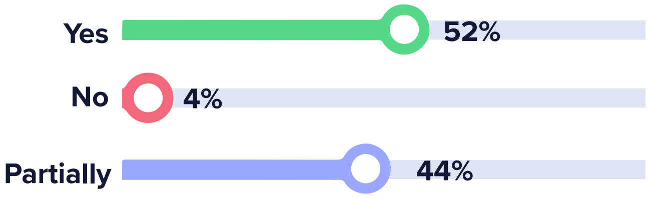
A number of banks want to use LLMs to help them to maintain the alignment between regulation, policies, standards, procedures, risks and controls. To check that alignment statically, they use the LLM to parse through their procedures and controls, then parse through what the regulators have provided, and then compare the two to ensure that they are accurately mapped.

A future development of this would then to be able to update the regulatory database and derive an instant gap analysis, using LLM to draft the policies and procedures necessary to fulfil any new regulatory requirement and in the future, using LLM to create the necessary controls and map them to the underlying risks.

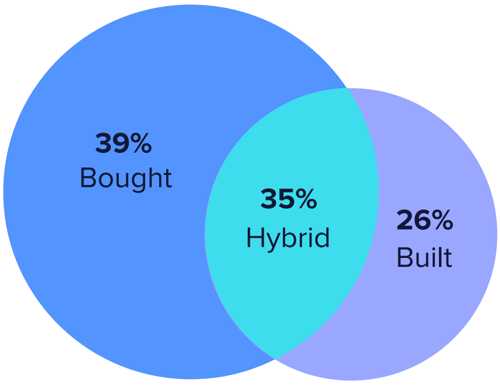
Another workflow-type use case would be in case management. Here generative AI could do the work of aggregating the datasets relevant to a particular alert and highlighting the key risk indicators in that data. It could even drive decisions around alert closing or escalation.

And another, easier, use case would be to use LLM-drive chatbots to be able to answer questions on policies or even questions around how to analyse alerts.

Are you satisfied overall with your case management / workflow tools?

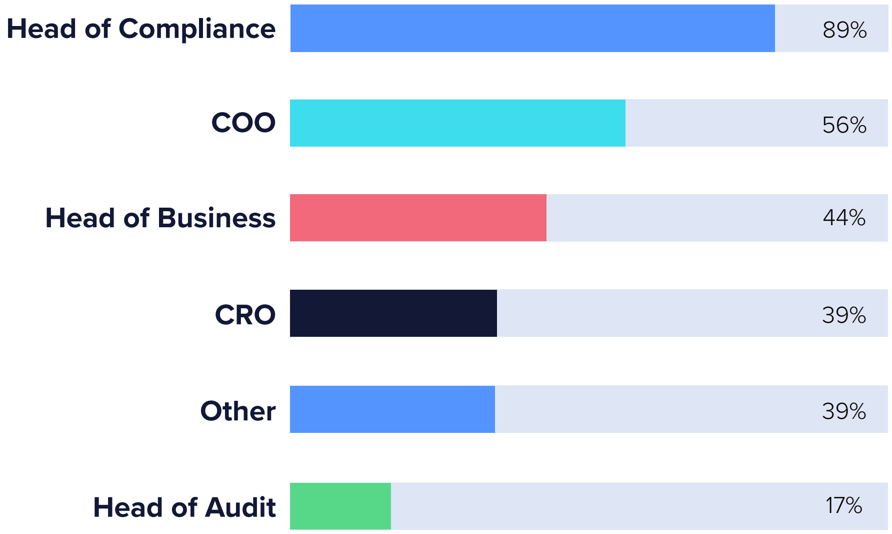


Have you bought or developed your own workflow and case management tools?



Surprisingly, given the problems that surveillance professionals describe in BAU, more than half the respondents were satisfied with their case management and workflow tools and just 4% were not.

Who are the enterprise wide stakeholders involved in external technology buying decisions at your bank?



Take the stakeholders with you

The broad picture of a sea-change in surveillance technology and a desire to invest is good news for surveillance professionals and also of course for the vendors.

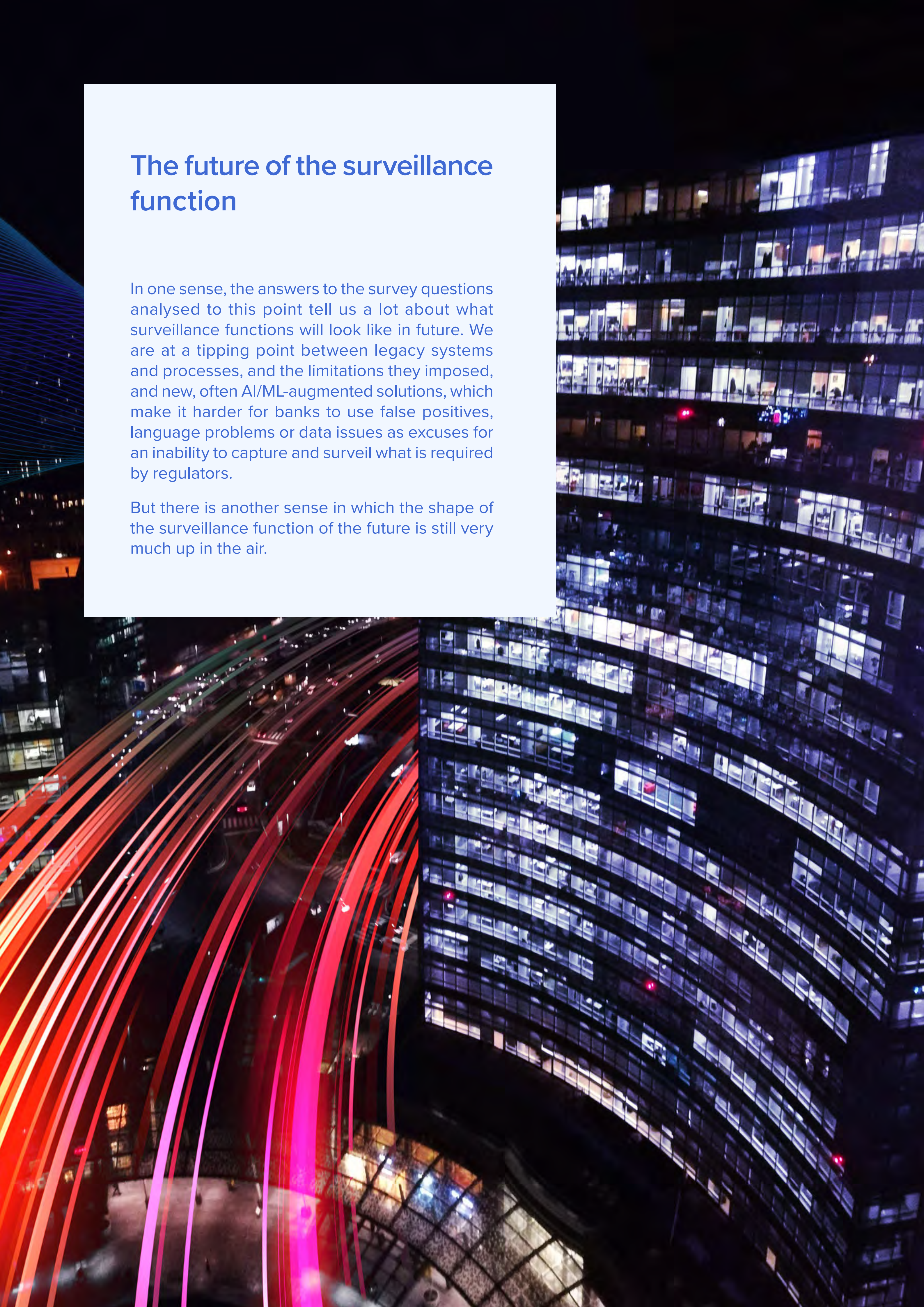
However, the technology procurement process in banks is not designed to give vendors or surveillance teams an easy ride. When asked who might be included in a group of enterprise-wide stakeholders in the technology buying decision for any new surveillance systems, the answers included the Head of Compliance, the Head of the Business, the COO, the CRO, the Head of Audit and ‘other’. When asked about the ‘other’, banks listed functions across IT including the CTO and Executives in finance.

It’s hard to see how procurement by a committee this large and diverse is the best way to stay agile in the face of rapid technology evolution. But technology vendors take note: helping compliance and surveillance heads win internal debates with these stakeholders, and persuading them of the benefits directly too, are the only way to make the case for new solutions.

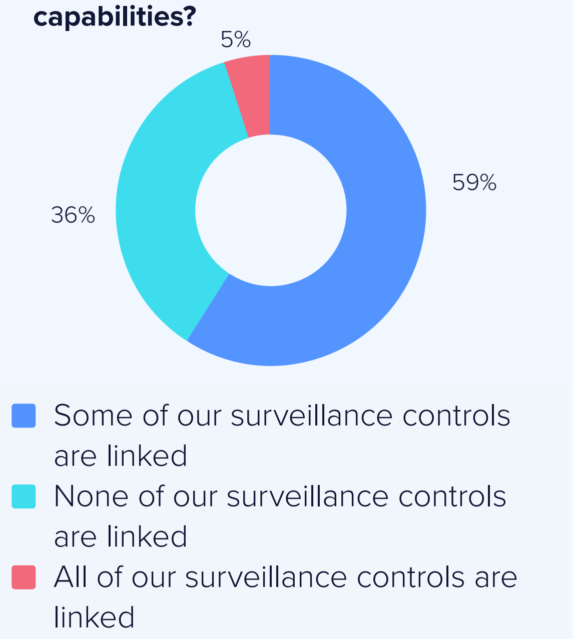
The future of the surveillance function

In one sense, the answers to the survey questions analysed to this point tell us a lot about what surveillance functions will look like in future. We are at a tipping point between legacy systems and processes, and the limitations they imposed, and new, often AI/ML-augmented solutions, which make it harder for banks to use false positives, language problems or data issues as excuses for an inability to capture and surveil what is required by regulators.

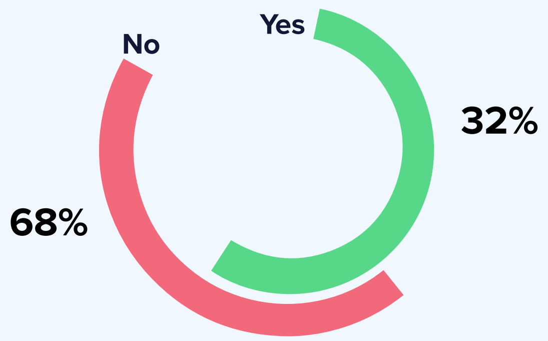
But there is another sense in which the shape of the surveillance function of the future is still very much up in the air.



How best describes the current state of your integrated surveillance capabilities?



Are your MAR surveillance functions organisationally being aligned with transaction monitoring functions in anti-money laundering (AML)?



Slow progress in contextual surveillance

For example, holistic/integrated/contextual surveillance has been a buzzword in surveillance for at least five years and describes a situation in which, at a minimum, all the comms and other information pertinent to a trade surveillance alert is available to an analyst at the moment they choose to review the alert.

In more utopian visions of this, technology would be able to assess these various sources and perhaps close the most obvious false positives while generating the documentary narrative explaining the review outcome.

Neither vision is remotely close outside a very small number of the largest global banks. In this survey, more than a third of banks admit that none of their surveillance controls are linked and just 5% say that all of their controls are linked.

This lack of progress is not simply down to technology or internal data aggregation obstacles – though these remain substantial issues. There is a more general strategic issue. Banks view trade, e-comms and voice surveillance differently, and in particular think of trade as a very separate discipline. Trade surveillance analysts perform a particular set of tasks and require a specific set of expertise around products and markets while comms surveillance is seen as more general and requiring fundamentally different analysis. It's hard to find banks truly committed to the idea of integrated surveillance or believing that it can bring sufficient benefits in efficiency and effectiveness to justify the costs.

A similar idea is that market abuse surveillance functions should be aligned in some way with the transaction monitoring function in AML. Again, superficially the concept is attractive: looking at client financial flows in conjunction with suspicious activity in banking and markets products could help identify financial crimes better, especially as some forms of market abuse are also predicate offences for financial crime.

But again, both technical and functional issues get in the way. Not all silos are bad or pointless fiefdoms. Silos are good structures within which to nurture and enhance specialist skills. The downside of this may be that some forms of collaboration do not make business sense. Certainly, almost 70% of banks do not think aligning surveillance with transaction monitoring (TM) is worth the effort at present, not least because there is no regulatory pressure to do so – as is also the case with integrated market abuse surveillance.

Is risk-based surveillance just too risky?

A more obviously valuable evolution of market abuse surveillance – and one publicly agreed by key regulators – is to move towards a more risk-based approach. The question though is what precisely this means in practice.

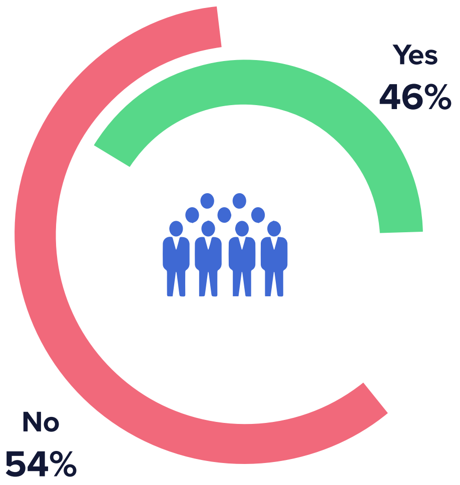
Does it mean that banks are allowed to devote resources only to those populations and product areas they themselves deem riskier, and can reduce or remove the surveillance of people who may be technically in-scope but whose ability to commit material market abuse is assessed as very low?

Does it mean that banks can leave low-risk channels out of their e-comms surveillance? Good news if they can, since the proliferation of venue-related channels, collaboration functionality and messaging applications is creating an unsustainable requirement to capture and monitor them.

And does it mean that banks should accelerate their efforts to risk-rank individuals – sometimes known somewhat controversially as trader profiling – again as a way of directing scarce resources to places where risk of misconduct is thought to be highest?

The basic answer to these questions seems to be ‘no’.

Are you moving towards a risk-based approach to surveillance and therefore not surveilling entire in-scope populations?



Risk-based surveillance scope

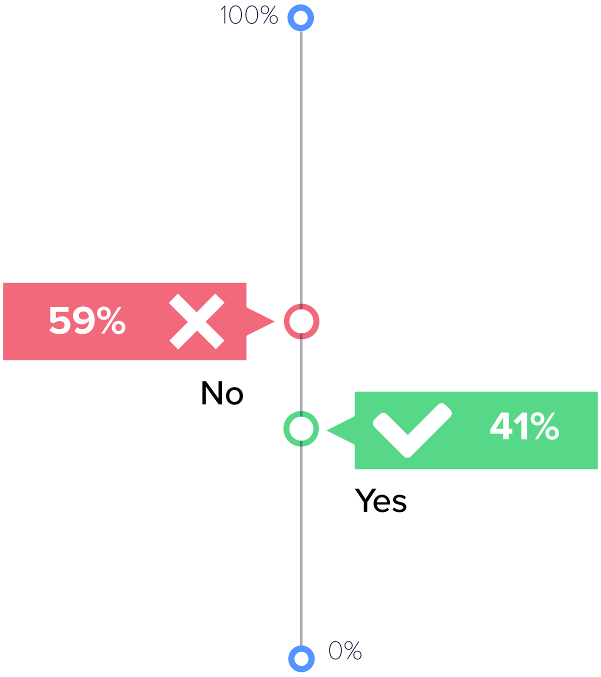
54% of respondents say that they are not moving towards a risk-based approach to surveillance with respect to in-scope populations. There is no obvious pattern to the responses – larger and smaller banks take both sides of the debate as do banks with more and less complex product suites.

The question forces the issue by asking whether people would remove people from the surveillance pool even if regulations deemed them to be in-scope. This might suggest that people suspect that regulators are less in favour of risk-based approaches than their public pronouncements indicate: if misconduct were found to have been committed by someone in-scope for surveillance but actually unsurveilled for risk-based reasons, do banks feel that the regulators would accept that?

When asked, banks don't claim that their lack of progress towards risk-based approaches reflects regulatory caution. 59% of respondents say that the risk of regulatory sanction is no obstacle to the adoption of risk-based surveillance.

However, the devil is in the detail. Half of those not moving towards a risk-based approach say that the reason for that is indeed the threat of regulatory sanction. But what about the other half? When asked they essentially say that the issue is certainty: it's easier to demonstrate compliance by mapping controls directly to regulations without any subjective, risk- based deviations that require additional explanation. There is also a question of maturity around risk appetite. Risk-based approaches imply a good understanding of where the risk truly lies in any given part of the business and a defined risk appetite that allows you to draw lines where you believe the risk is unacceptable and acceptable. In non-financial risk management, where much of the time the risks are high-impact but very low probability, that kind of approach is analytically very difficult.

Does the risk of regulatory sanction limit your bank's ability to move at pace to a more effective, risk-based surveillance?

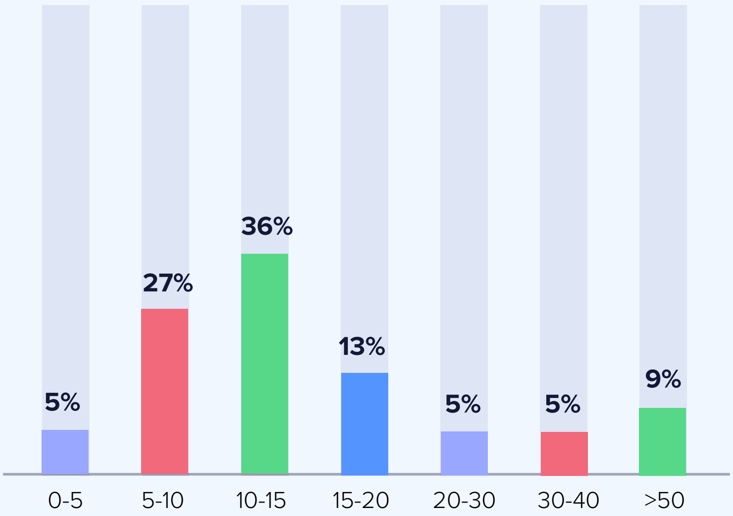


Risk-based surveillance scope

That said, risk-based approaches are being adopted around e-comms channels, at least according to the interviews conducted around the survey. The challenge in e-comms is clear: banks are surveilling anything between 0-5 and over 50 communications channels. So how do they choose? And what happens as the total number of possible channels to monitor keeps rising?

Here banks say that it is unsustainable and pointless to not take a risk-based approach. So, public chat functions are not monitored on the assumption that no-one would attempt to communicate misconduct on a medium everyone can see. Internal but public collaboration channels would be treated in the same way. Chatbots that can only respond in a given, pre-determined way would not be surveilled. And on-venue communications channels not designed for text-based communications would also be excluded. Essentially, only private, bilateral channels designed for communicating would be surveilled.

How many e-comms channels are you monitoring?



Using trader profiling to match resources to risk

Potentially the most significant development in risk-based surveillance is the idea that risk is a function of the individual. Proponents of trader profiling argue that banks conduct surveillance for two main reasons: to comply with regulations designed to protect market integrity and to protect the banks from the damage bad employees can cause both through committing market abuse and more broadly through their behaviour.

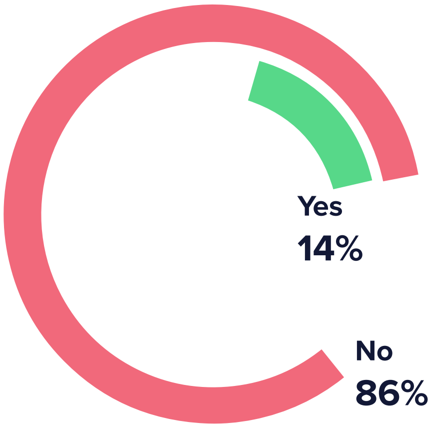
In both cases, they say, it makes sense to use all the data at their disposal to direct surveillance at those individuals whose behaviours suggest they are more likely to break rules or act counter to their organisation's cultural values.

"We now have data on both people's specific work performance – so detailed profit and loss (P&L) analysis and trade booking behaviour for a trader for example – and on their cultural behaviour – breaching remote working rules, failing to do mandatory training, bad language in emails – and if you find that there are repeated breaches of your standards then that's the person that you're probably more likely to have a problem with," said one participant in favour of trader profiling. "This is really what I think of as holistic surveillance, rather than the aggregation of voice, e-comms and trade. I think of it as profiling behaviour and that that will create the alerts of the future."

So, is trader profiling part of the surveillance function of the future? Well, 86% do not use it and when asked, they seem surprisingly hostile to the idea. The main reasons given for not doing it are ethical and legal. In Europe, there is still a perception that data privacy laws stand in the way of this kind of surveillance, though it is hard to find the exact clauses that say this. Workers' councils and in-house legal teams certainly fight this kind of monitoring too.

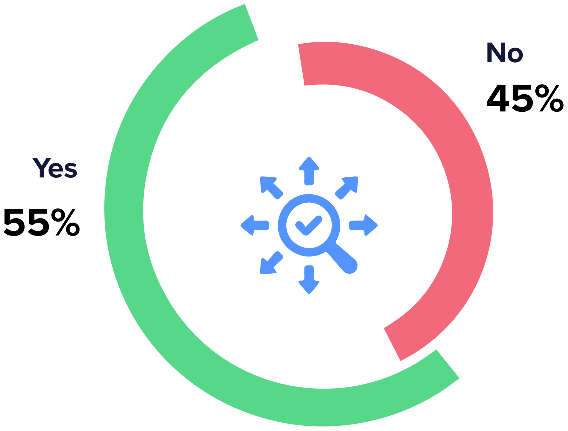
But even in the US, where the legal obstacles are few, banks are surprisingly resistant to the idea of assigning riskiness to individuals outside very narrow employee-performance assessments. There seems to be a fear that this level of monitoring is fundamentally wrong and that it sends out a damaging message that the firm mistrusts its employees. Given the monitoring practices in other industries, it is hard to understand why banks feel that they are so different.

Do you use trader profiling to filter your alerts?



Model risk management: the future is now

Are the calibration of your models formally approved by a MRM forum?



Those on the other side of the argument say that model risk analysis is not designed to examine whether surveillance models work or not – in the sense of actually detecting risk.

One trend that is already defining the surveillance function of the future is the relentless march of MRM/ governance. Just a couple of years ago, surveillance scenarios would not have met most people's definition of a model, and even if they had, they would not have had to be pored over by the type of quants whose job used to be to work out whether trading algorithms were working as designed.

Today, the regulators have weighed in and banks have followed their lead. More than half of the respondents say that calibration of their models is now formally approved by an MRM forum of some kind. Whether or not they think that this adds any value or mitigates any more risk is another matter.

Some do not believe that surveillance 'models' are models at all. A model takes some value (or set of values) as input and produces some value (or set of values) as output via a defined set of computations. The kinds of rules-based logic used to generate surveillance alerts does not seem to them to be complex enough to meet a sensible definition of a 'model'.

Even those who agree that some computations done in surveillance can be seen as models, still see model risk governance by quants used to looking at financial risk algorithms as pointless.

One sceptic put it like this: "No surveillance model parameter change is going to expose a bank to immediate loss because no 'model' in any 3 lines of defence context is connected to anything except an alert. So, the output isn't a trade, or a risk position, or a direct action in a market of any kind. All that happens if you alter a surveillance 'model' is that different alerts are generated. Now given that 99% of alerts generated are noise anyway, one does not need teams of quants arguing the toss about each change and how that change alters the output risk, because they have no way of telling that. It is impossible to measure non-financial risk quantitatively, so even if control systems for financial risk had direct, measurable effects on the underlying non-financial risk (which they don't) you still cannot say anything quantitative about their effect on (the still unmeasurable) non-financial risk. And as I said, in any case, the models only generate alerts. So, applying the full might of teams whose job it is to work out what happens if a complex trading algorithm goes rogue to a surveillance calibration is beyond stupid."

Those on the other side of the argument say that model risk analysis is not designed to examine whether surveillance models work or not – in the sense of actually detecting risk. MRM teams simply look at the models and determine that the calculations do what they are designed to do. In this role, they are discovering that some surveillance calibrations do not, in fact, do what the surveillance teams designed them to do.

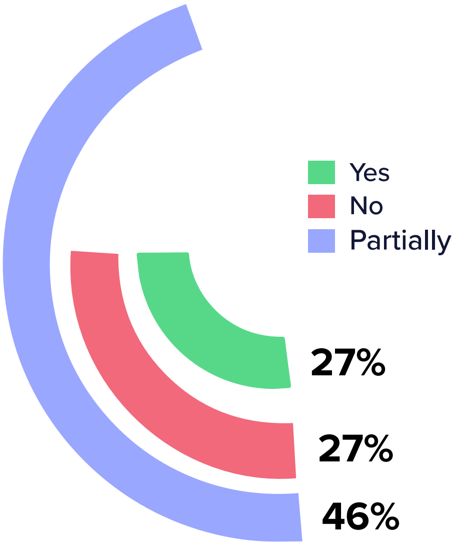
Either way, it's clear that the future surveillance function will endure more, not less, model risk analysis.

The future is cross-product

Another trend that is all one way is the continued development of cross-product market abuse. Again, accelerated by regulatory pressure, banks have had to confront the much more difficult problems associated with detecting misconduct achieved through the use of related products. Detecting cross-instrument, cross-asset class and cross-venue manipulation – and discriminating between manipulation and hedging – is one of the most challenging tasks for surveillance teams today. It requires new technology, the acquisition and aggregation of difficult-to-obtain order and quote data, understanding of complex correlations between instruments and markets, better understanding of individual traders' P&Ls, and people with the trading knowledge to understand how this kind of manipulation is executed in practice.

The good news is that more than a quarter of respondents now have the ability to surveil for cross-product market abuse. However, that leaves 73% needing to upgrade their capabilities or start from scratch. More technology, more data re-engineering and more people will be necessary.

Do you have the ability to surveil for cross-product market abuse?



A never-ending story

The big picture message of this survey is that surveillance for market abuse, conduct and culture is never 'done'. The evolution of products and venues requires upgrades to trade and comms surveillance. The sophistication of new tools and technologies allows banks to detect and analyse scenarios that were previously impossible. New communications analysis solutions allow banks to translate, transcribe and monitor communications that could not be processed economically except via tiny samples.

In addition, the regulatory landscape is never static. Regulators introduce new rules. More often they emphasise existing ones and focus on areas where they perceive banks are failing to mitigate risk properly. So, we have seen them look at messaging, cross-market abuse, failure to fully capture venue data feeds into trade surveillance, trade surveillance calibration failures and model risk governance, for example.

And we have seen banks show caution around, for example, the adoption of AI and risk-based approaches to surveillance, because of what they perceive is regulatory risk, despite regulators themselves saying that they favour both the adoption of new technology and the use of those risk-based approaches.

The power of regulation to shape banks' responses in market abuse surveillance will continue – as emphasised by the FCA's latest consultation document published on 27 February 2024.

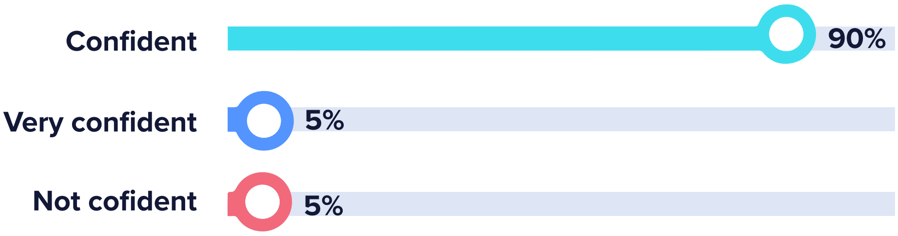
This sets out a new approach where for the first time, the regulator will identify firms and individuals under investigation. In a jointly written foreword for the document, Joint Executive Directors of Enforcement and Market Oversight, Therese Chambers and Steve Smart, summarized the rationale for this shift.

"Enforcement action is not simply about individual instances of punishment. Its greatest impact is as deterrence, and in educating the whole market on what we expect, and where others have fallen short. By being clearer about the types of misconduct we think warrant a formal investigation, it allows other firms to learn lessons, raise their standards, and think twice about doing the same at a much earlier stage than currently."

Similar to the Security and Exchange Commission (SEC) outlining the 'trigger factors' that will lead to the regulator investigating Chief Compliance Officers, this new transparency is intended to give firms and individuals clear oversight of what might lead the regulator to come knocking.

Despite the many gaps revealed by the survey responses, and despite that regulatory tone, 90% of banks are confident that their surveillance functions are effective enough to detect potential future cases of market abuse.

How confident are you that your surveillance function is effective enough to detect potential future cases of market abuse in your bank?

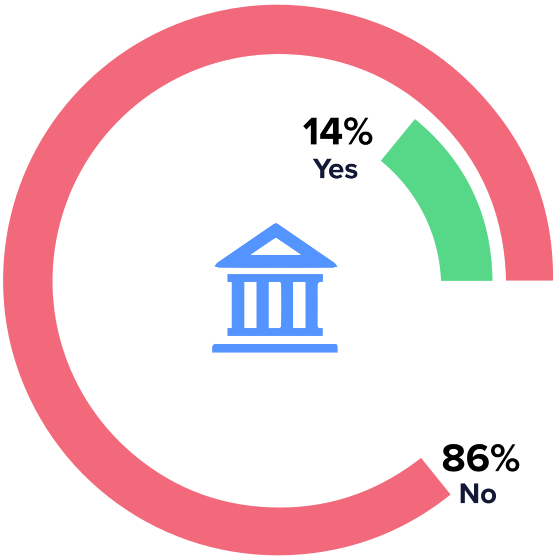


If there is any bad news in the survey it is that progress away from a regulatory compliance mindset is slower than many would like. We see how banks are not moving particularly quickly towards integrated surveillance or the alignment of surveillance and AML. We see that investment in CTB projects related to surveillance could be higher. And we see in the final graph that just 14% of banks are using their surveillance capabilities to identify commercial opportunities in their client, market and trading data.

This is a missed opportunity and it shows how far we still have to go in moving away from the idea that surveillance is simply an unavoidable compliance cost. If the business could be persuaded of the potential profit embedded in surveillance data, then many of the enterprise data and organisational issues that dog surveillance would start to be solved.

In the meantime, there is plenty of work to be done, and money to be spent, just ensuring coverage and using new technology to transform the detection of misconduct and the analysis of the alerts surveillance systems generate.

Is your bank using your surveillance capabilities to identify commercial opportunities in your bank's client, market and trading data?



Smarsh enables companies to transform oversight into foresight by surfacing business-critical signals in more than 100 digital communications channels. Regulated organisations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisors and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com.

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions.
You must consult your attorney regarding your compliance with applicable laws and regulations.

Report - April, 2024

☎ 1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh