PwC Market Abuse Surveillance Survey 2019

March 2019

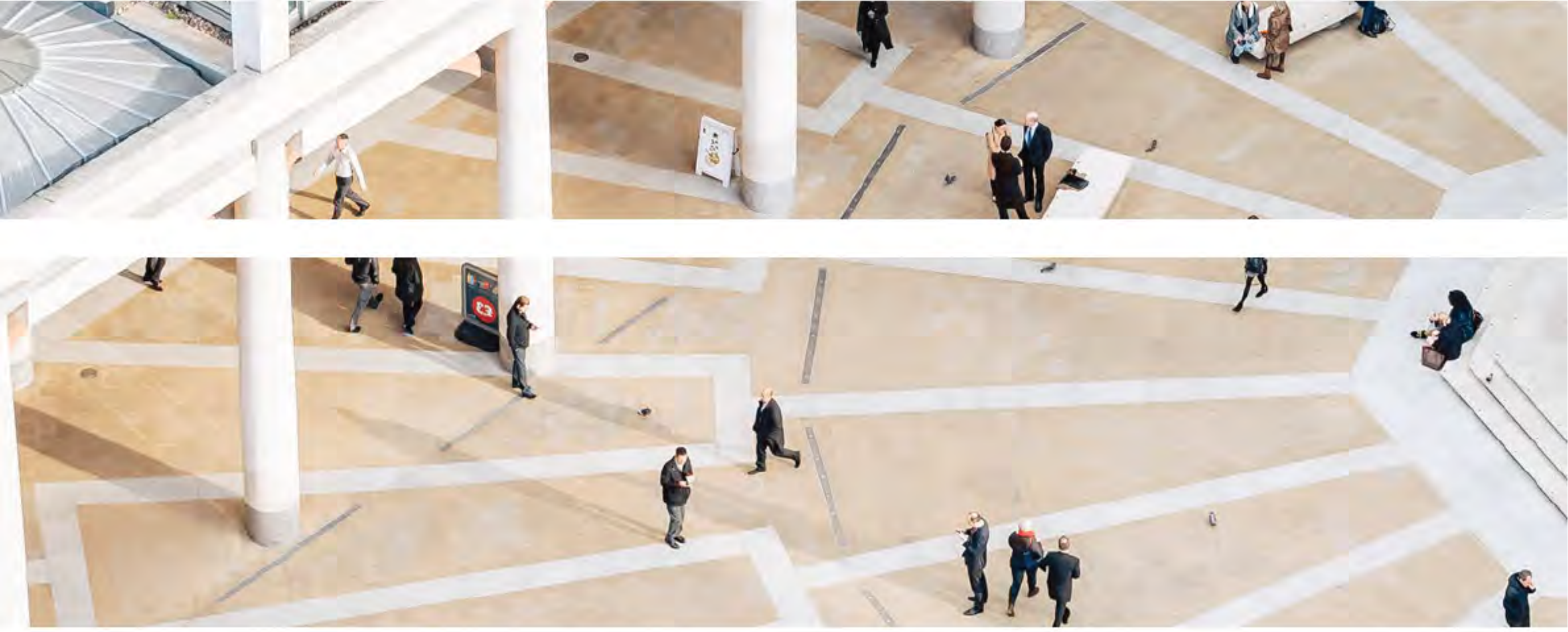
Introduction

We last carried out our Market Abuse Surveillance Survey at the beginning of 2016, shortly before the EU Market Abuse Regulation (MAR) went live. At that time, organisations were working to understand the expanded regulation's impact on surveillance given the requirement to implement adequate systems and controls to prevent and detect market abuse.

While we considered running the survey again in 2017 and 2018, we felt that not enough had changed since 2016 to give a meaningful view of the direction of travel. Three years on, having observed more significant changes in the ways organisations are approaching surveillance, we felt that the time was right to re-run the survey. Undoubtedly, the maturity of banks' surveillance functions has increased considerably over the last three years.

This report summarises the key themes emerging from the survey as well as our views on the difficulties we observe in establishing effective surveillance. We have sought to pose questions to the industry to provoke debate where we have observed challenges that remain unresolved.

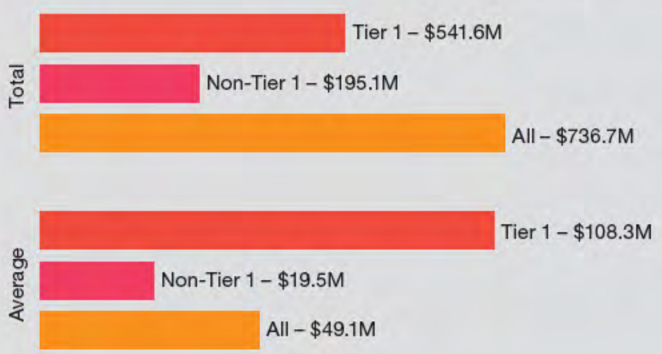
Contents



Part 1 – Perspectives on the evolution of surveillance since 2016

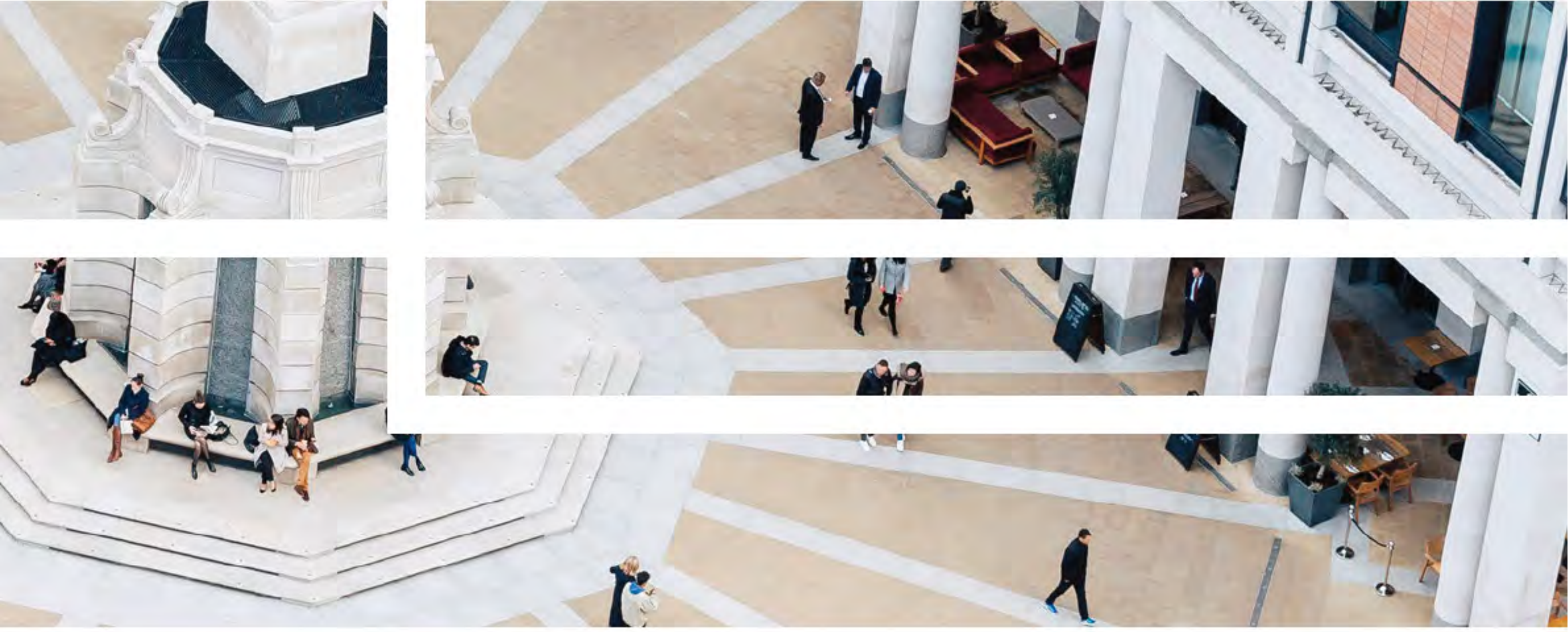
How much progress has surveillance made since 2016?

Figure 1: Surveillance spend over the last two years



In our 2016 Surveillance Survey we concluded that 'Surveillance has yet to deliver as a fully effective tool for preventing market abuse in financial markets. That's largely owing to limitations in technology and a lack of clarity about optimal organisation of responsibilities and activities. But the stakes are too high for the banks to do anything other than invest further and rely on emerging technologies to plug the gaps'.

Three years have passed since then, and it's clear that the discipline of surveillance has undergone an evolution and that this evolution remains dynamic and as yet incomplete. Additionally, the pace of change is accelerating. Operating models are evolving, a new generation of surveillance technologies have established a market presence and areas of surveillance previously believed to be too difficult are now becoming established practice.

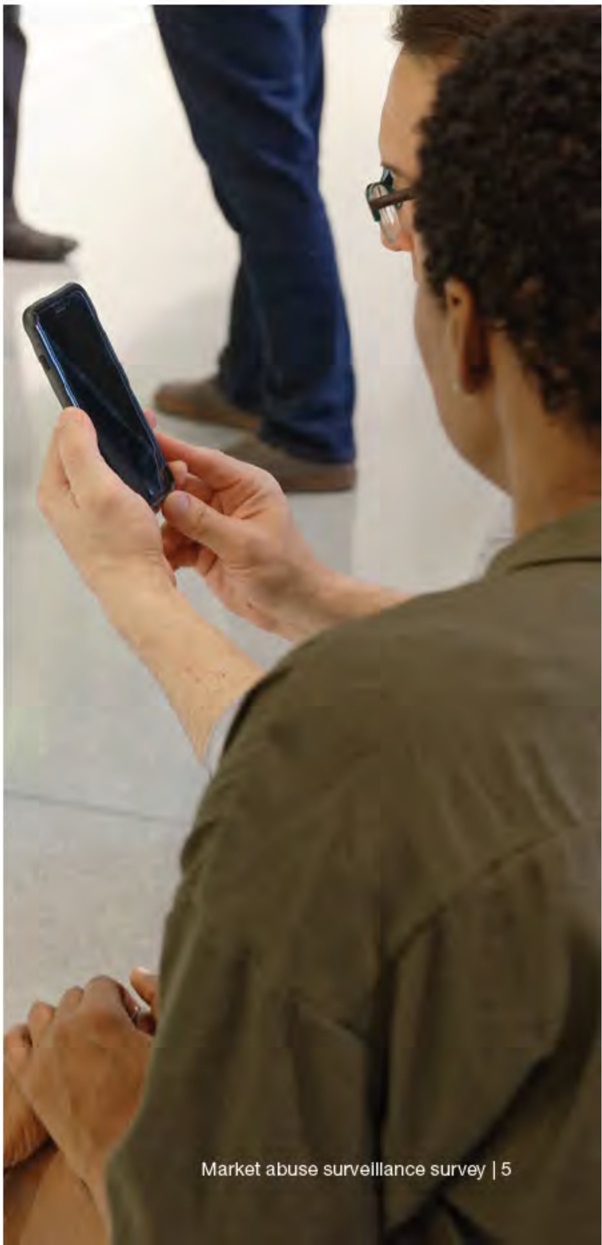


> $737m – Spend on surveillance in the last two years[2]

> 20 of the 21 surveyed banks believe their surveillance is more effective than in 2016

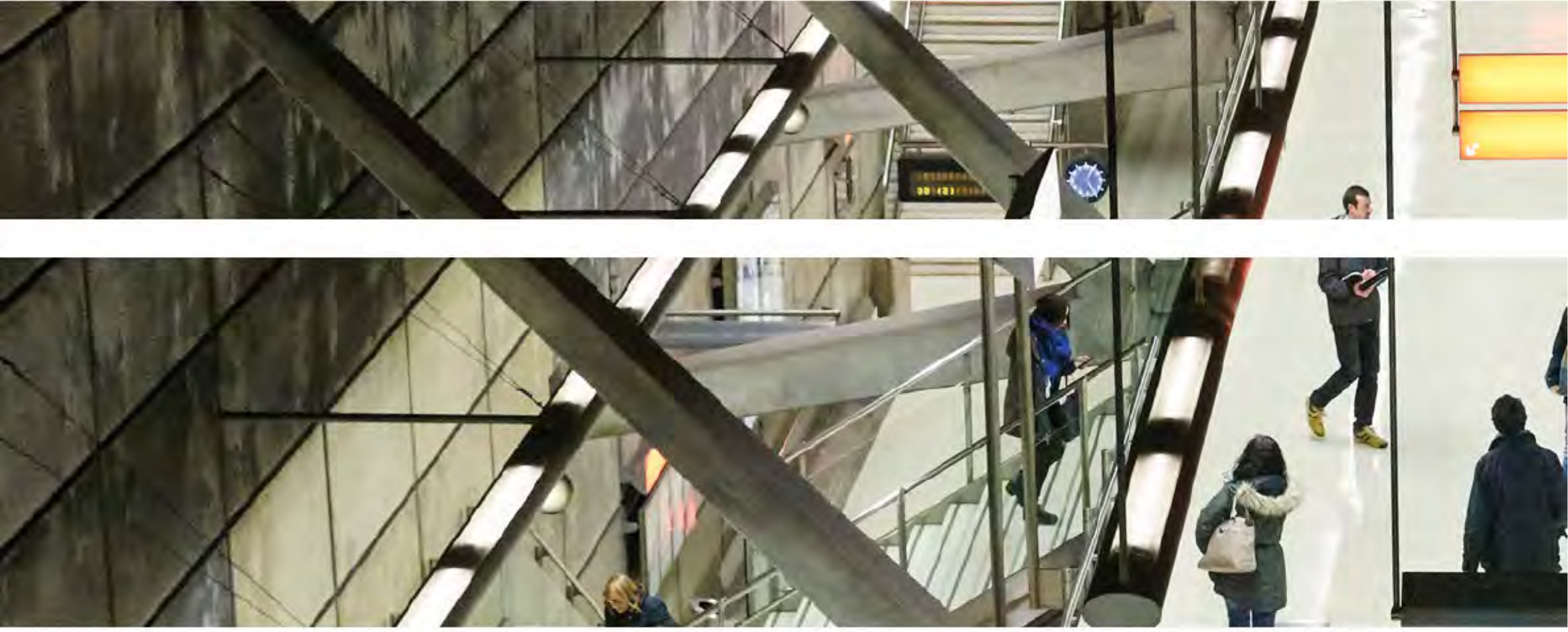
In short, the surveillance industry is maturing, driven by significant levels of investment. The participants of our 2016 survey told us that they expected to increase their investments in surveillance solutions substantially, with the majority projecting between $6.5m and $13m[1] in additional spending over a 12-18 month period. This has certainly proved to be the case, and is supported by the statistic that in the last two years the surveyed banks have spent $737m[2] (15 participants) developing and enhancing their surveillance capability. Since 2016, the survey participants have implemented 25 vendor solutions (excluding in house developed solutions), driven by a desire to increase both the capability and coverage of their surveillance.

Therefore not unsurprisingly, the industry is positive about the levels of progress that have been made. This sentiment is reflected in the belief of 20 of the 21 surveyed banks that their surveillance capability is more effective than it was in 2016.



[1] In 2016 this was reported as 5-10m GBP which was converted to 6.5m-13m in USD today. Values were converted from local currency to USD using Bank of England exchange rates on 19 February 2019.

[2] Of the 21 participating banks 15 provided data on historical spend. Values were converted from local currency to USD using Bank of England exchange rates on 19 February 2019.



How important is it to have a comprehensive market abuse risk assessment?

A comprehensive market abuse risk assessment is the cornerstone of effective surveillance. It forms the foundation for developing a successful surveillance function, ensuring that the surveillance undertaken is instructed by how market abuse could crystallise in the business, and dictating the size and scale of the automated surveillance needed.

Participants to the survey have constructed a market abuse risk assessment to inform senior management of how market abuse could manifest and to set out why they have elected to manage market abuse risk through preventative controls or detective surveillance across the lines of defence.

However, there doesn't appear to be a common standard adhered to across the banks for the creation and maintenance of market abuse risk assessment, despite the fact this is a clear area of regulatory interest. There is a lack of common templates and approved methodology, which may result in inconsistencies in the risk assessment inputs and outputs across banks. In addition, the granularity required to perform a robust market abuse risk assessment varies across participants with assessments variously performed at an asset class, product and sub-product level.

Each approach has its advocates and while it's difficult to pronounce one approach to be right and the others to be wrong, it's worth considering that a more granular risk assessment will better support the process of selecting trade surveillance scenarios and calibrating distinct instances of these to better reflect the risk profile of the business. This is an area which will continue to evolve and participants feel that they would benefit from more regulatory pronouncements, with a number of participants citing the recent series of the UK FCA's Market Watch newsletters as particularly informative when enhancing their market abuse risk assessments.

The focus on market abuse risk assessments is likely to increase rather than dissipate over the short to medium term, given the significance placed on being able to demonstrate a clear lineage between the crystallisation of risk in the business and the surveillance in place to mitigate this risk. What is certain is that the appreciation of risk is fundamental to the operation of effective surveillance.

To what extent have surveillance operating models evolved?

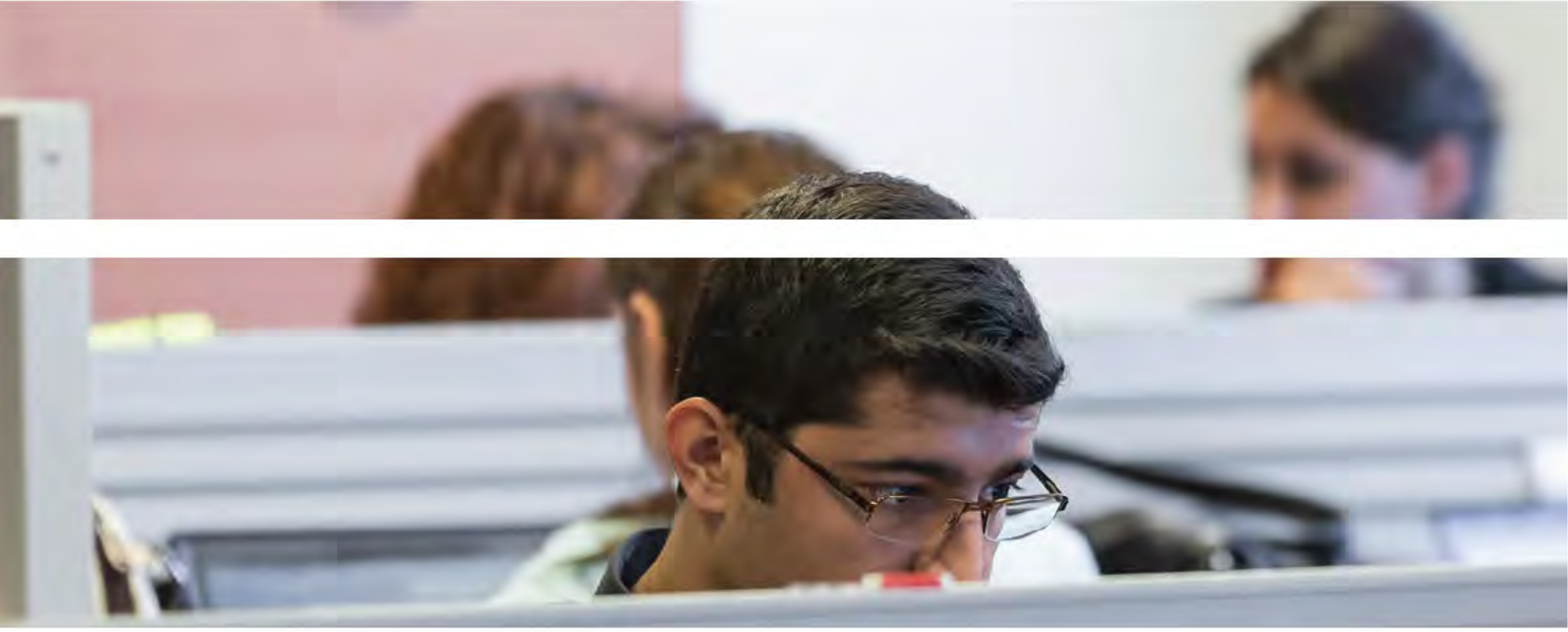
In the 2016 survey, 45% of participants reported that their surveillance functions resided or partially resided in the front office. Banks were taking steps to transfer more responsibility into the first line, combining technology and knowledge of the trading environment to identify market abusive events more readily.

In the intervening period a debate ensued between banks and regulators as to whether first line surveillance functions can be truly independent. The 2019 survey suggests that the question about where surveillance should primarily reside within the organisation has now been overwhelmingly settled, as 18 of the 21 banks surveyed now have surveillance situated fully or predominantly in the second line.

Figure 2: Where does responsibility for surveillance reside in 2019?

Near and off-shoring models remain prevalent with a number of centres being used for the review of trade, eComms and voice surveillance. The majority of the banks use near and off-shore locations to conduct 'Level 1' alert review with further levels of escalated review conducted by skilled on-shore surveillance practitioners. However, there is a move towards conducting more varied near and off-shore roles to encompass more levels of alert view. In part this step is designed to increase staff retention rates.

Given the escalating levels of investment, both operational and capital expenditure, in the last three years, we might have expected to see increased levels of surveillance out-sourcing as a means of delivering cost reduction, and achieving more with less budget. However, to date only two banks undertake any material level of out-sourcing, both in relation to review of their alert population. It will be interesting to observe the extent to which the industry adopts outsourcing and whether the banks can get comfortable with the risks inherent in third parties performing a level of surveillance on their behalf. Equally to what extent might global regulators be comfortable with this approach?



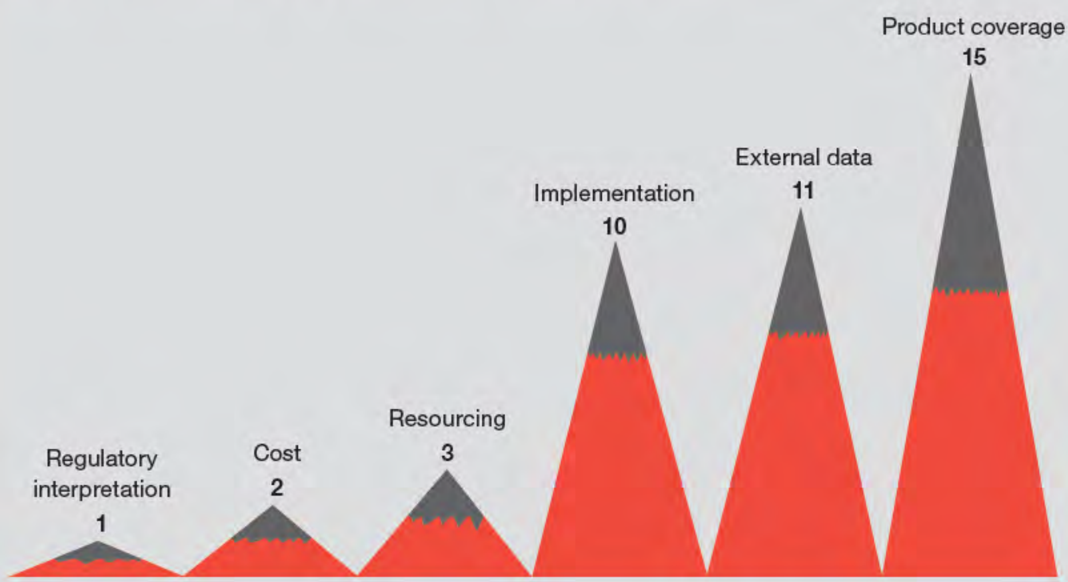
Challenges for the industry – Can the MAR mountain be scaled?

MAR is the most prescriptive international regulation on market abuse and consequently represents the greatest challenge for international banks in terms of compliance. As such, almost three years after it went live, survey participants are still grappling with elements of the regulation. The sheer breadth of MAR has proved a challenge for all.

The challenges the banks still face with implementing MAR are myriad. Providing surveillance over all products remains the area of greatest difficulty. 15 of our survey participants noted that they were working to address coverage gaps, with quote capture and fixed income frequently cited as the areas of continued focus.

Challenges monitoring for abuse through trading of more complex structured products was also reported as an area where market practice was yet to emerge.

Figure 3: What are the key challenges in complying with MAR?



What is clear is that achieving MAR compliance is not easy, despite the heavy investments made by the majority of survey participants since the inception of the regulation. MAR compliance entails achieving a measure of success across many surveillance dimensions. And it's apparent that there is a time lag between making investments in surveillance and realising the benefits of doing so. 10 participants highlighted the difficulties inherent in implementing surveillance technology, while complexities of data, recruitment and budgeting and investment were noted by others. The size of the MAR mountain remains daunting and successful paths to the summit are not yet well trod.

As a consequence participants also expressed a view that greater clarity from regulators as to what they expect would help focus prioritisation of effort more effectively. The need for clarity is made more acute by the strong sense amongst participants that the regulatory bar is going up with growing expectations, particularly around trade and order surveillance product coverage.

It's clear that participants have strongly committed to attaining compliance with MAR and real progress has been made since 2016. As a result a majority of participants are robust in stating that their market abuse controls place them in a defensible position with regulators, but there is widespread acknowledgement that more needs to be done to scale the MAR mountain.

Part 2 – Perspectives on the challenges of performing effective surveillance

What happened to holistic surveillance?

Our 2016 survey called out 'holistic surveillance' as the key development that organisations wanted to see in the future. In 2016, 12 out of 20 banks reported it as one of their top priorities. There was a sense of optimism that holistic surveillance was not only very achievable but also 'just around the corner'. The term 'holistic surveillance' was on everyone's lips and the future felt bright.

Over the last three years reality has bitten. Performing effective surveillance over one channel (e.g. trade, eComms or voice) has proved difficult enough, and so the enthusiasm for combining both structured and unstructured data from multiple disparate systems has tempered somewhat.

As surveillance functions have matured, so too has the understanding of technical complexities with surveillance. Reality has replaced hype; 'Minority Report' style analytics giving way to the attritional nature of identifying and addressing data challenges. Participants noted disparate data, limitations to existing technology, data latency and accessibility as barriers to conducting holistic surveillance.

However the goal of achieving holistic surveillance has not died. It has reincarnated in a slightly different guise, reborn as 'integrated surveillance'. Integrated surveillance is about taking a pragmatic, practical and cost efficient set of steps to seek to achieve something closer to a 360° view of trading behavior and the associated risk of market abuse. Advocates of integrated surveillance recognise that data will always be imperfect, that combining data forms and types is hard, and that ultimately even if it were possible to do so there is no guarantee of being able to identify a 'signal through all the noise'.

There is a school of thought that integrated surveillance can be partially performed by a more manual joining of the dots. And as such there is a growing trend to place greater reliance on processes and organisational structures. A number of banks are aligning their teams on products rather than surveillance channels so that individual analysts might review trade, eComms or voice alerts relating to a specific trading desk in a given day. Additionally, case management systems are being used as an integration proxy.

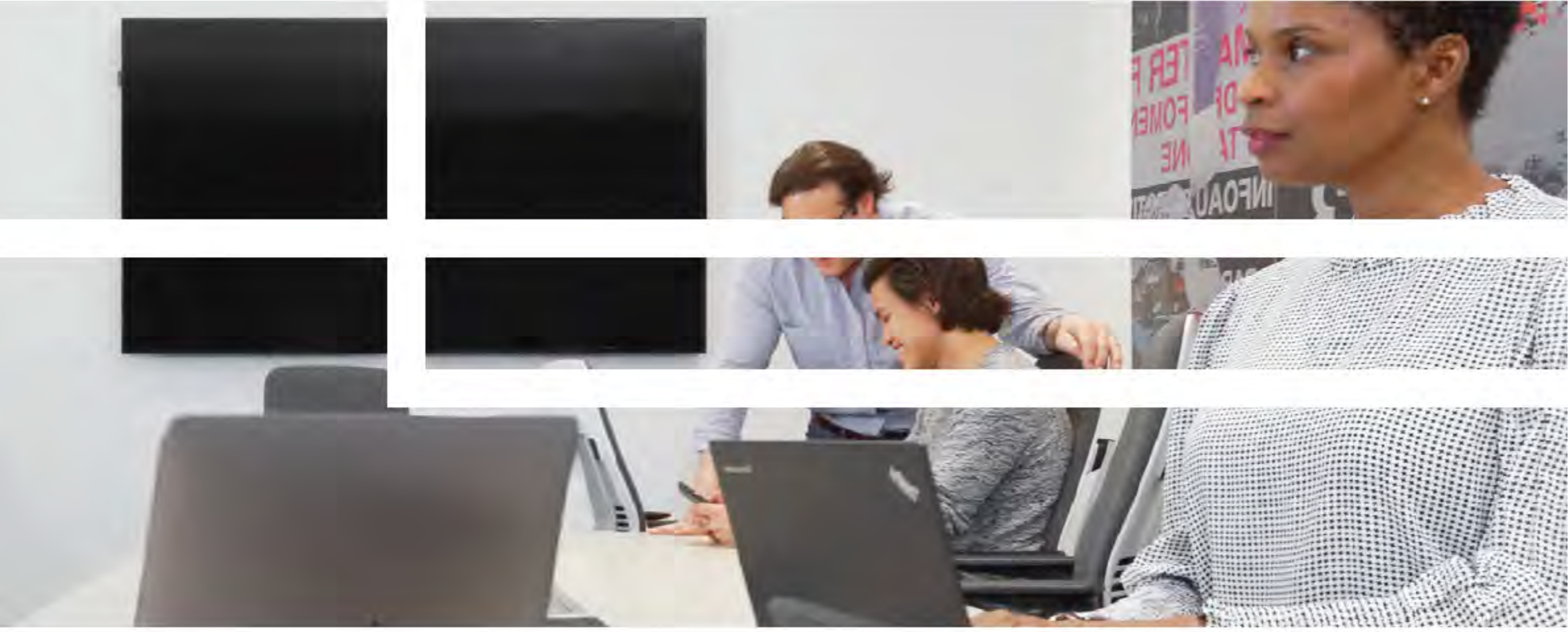
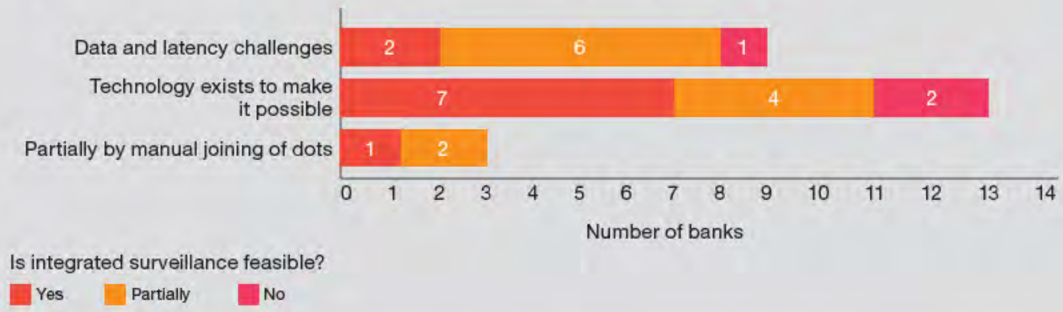


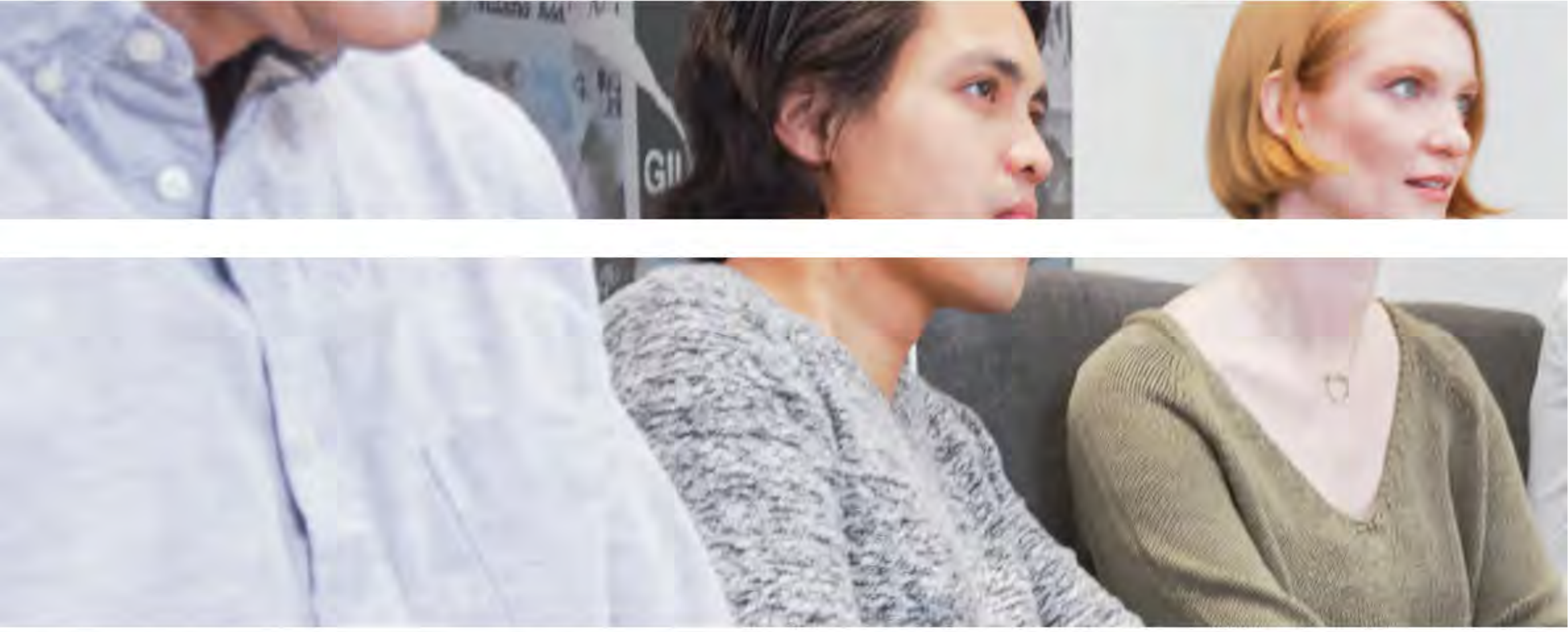
Figure 4: Views on the feasibility of achieving integrated surveillance



Until such time as further technology advances are made, integrated surveillance needs to rely more on the virtues of humans, rather than machines. This view is borne out by the fact that while 45% of participants believe that integrated surveillance is possible, 35% believe it is only partially feasible with 20% believing the obstacles to ever achieving it are too numerous.[3]

Arguably none of the survey participants has yet achieved this goal although some have taken steps on the journey. For now integrated surveillance remains an aspiration.

[3] Of the 21 participating banks 20 provided an answer as to whether they believed integrated surveillance was feasible.



Effective surveillance – How important is getting the data right?

Arguably the single greatest obstacle to the 2016 ideal of 'holistic surveillance' has been the issue of data. Provision of good management information and insightful analytics is not possible without clean and accurate data. The existence, completeness and accuracy of data and the ability to bring it together is a prerequisite for effective surveillance, and is a subject that survey participants are all grappling with. Data quality is not an issue reserved to surveillance alone, and is as relevant to the challenges of complying with MiFID 2 as it is for MAR.

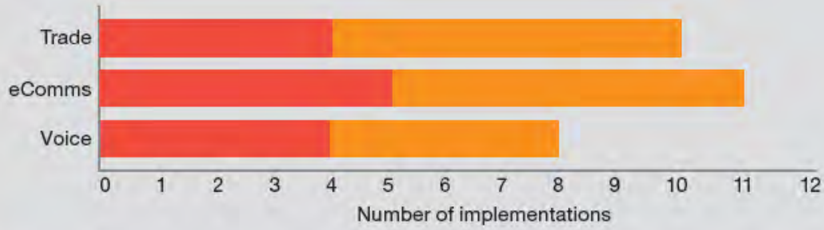
For heads of surveillance today it's a truth universally acknowledged that good data is the key to performing good surveillance. 17 participants cited data as being a greater issue for effective surveillance than software. Challenges noted included data sourcing, integration complexities, cleansing issues, usability issues due to the disparate nature of the data and the sheer volumes of data that are produced. Sourcing of external market data emerged as a particular concern with 11 banks stating that this was one of their greatest challenges, typically in combination with obtaining surveillance product coverage. Data capture is the principal obstacle to the industry problem of providing surveillance over orders and quotes.

Logic would dictate that the importance of data for surveillance will only increase. The continued expansion of e-trading means that surveillance functions will need to be able to monitor increasing volumes of data in low latency markets. Nonetheless participants are cautiously optimistic with 12 banks expressing a view that the industry can keep pace with the onslaught of data. Only time will tell if this confidence is well placed.

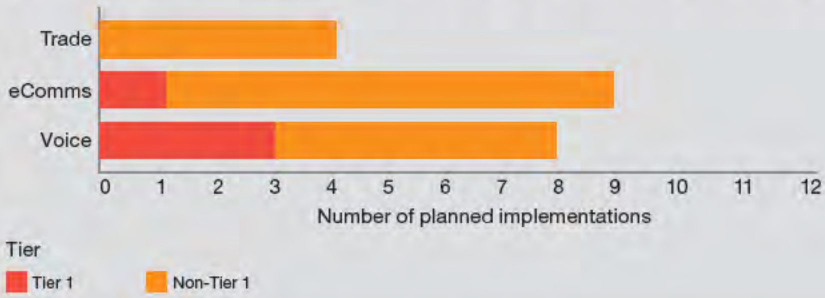
When will the proliferation of vendor implementations end?

Figure 5:

Number of implementations since 2016, by surveillance channel and tier



Number of planned implementations, by surveillance channel and tier



When we undertook the 2016 survey a number of banks were undertaking vendor evaluation exercises, with yet more adopting a cautious 'wait and see' attitude as they sought to discern which vendors would gain market share and widespread adoption.

In the period since, banks have made substantial software investment with 17 survey participants having implemented solutions.

The sheer scale of the banks' response to MAR is illustrated further by the number of planned investments in software in the near future. There are plans for a further 21 software implementations; nine for eComms, eight for voice and four for trade surveillance.

This investment reflects a mix of system replacement, particularly around eComms, and a desire to acquire additive or enhanced capability.

What is clear is that the Tier 1 banks have already made substantial investment and have implemented or are in the process of completing implementation of their chosen vendor software. By contrast the non-Tier 1 banks are planning further augmentation of their surveillance capability with an appetite to embrace voice surveillance and are considering deployment of new eComms technology. 17 of the potential future software implementations will be undertaken in non-Tier 1 banks.

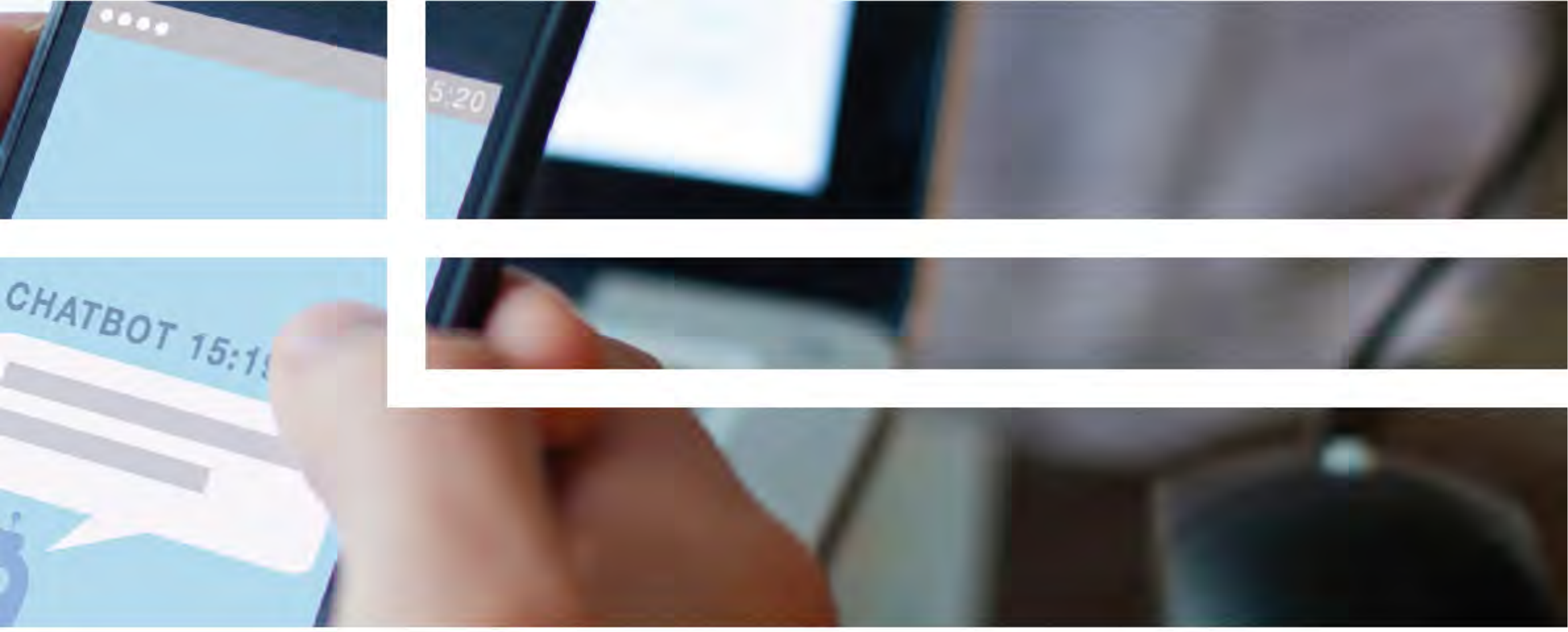
Choice of surveillance vendors – Has there been convergence or divergence?

Navigating the vendor landscape to procure the best fit solution is always challenging, and in the case of surveillance has been exacerbated by the proliferation of software vendors with solutions. The banks have frequently expressed a desire for a clear and de-risked set of choices to emerge; the ability to seek comfort in making a software selection embraced by a majority of their peers. In 2019 are we any nearer to this situation?

The answer is more nuanced than a simple 'yes' or 'no'. Increasingly there is a consensus amongst the banks that eComms solutions using some form of NLP (natural language processing) technology represent a future they wish to pursue and consequently a large percentage of market share has been achieved in the period 2016-2019 by those vendors employing this technique.

Across the discipline of trade surveillance, several established vendors have a large market share, based upon historic strengths providing surveillance over equities. But given the propensity for our participants to have multiple trade surveillance solutions there are a number of other solutions being used to monitor FX, Fixed Income and Commodities. A number of vendors have a footprint, with no one vendor having achieved a dominant market share. In the emerging theatre of voice surveillance no leader has yet emerged.

A discernible pattern of choice has emerged across the Tier 1 banks and while it would be overly simplistic to state that they are running an identikit software strategy, there is commonality of approach and a number have deployed or are deploying the same eComms and trade surveillance technology. It remains to be seen whether this will provide a blueprint for the non-Tier 1 banks to follow.

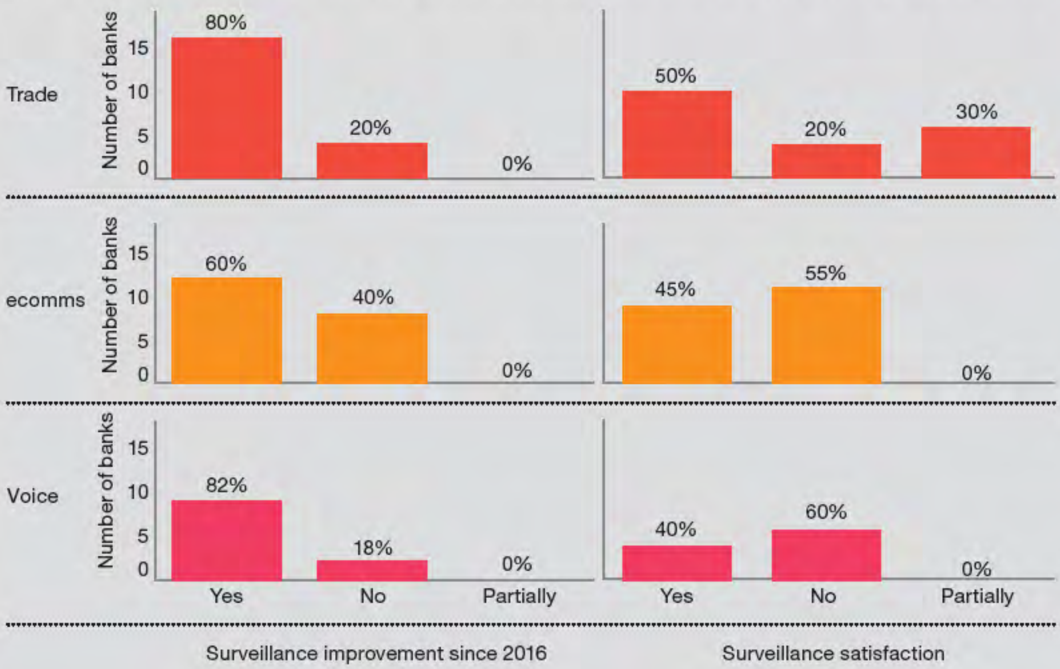


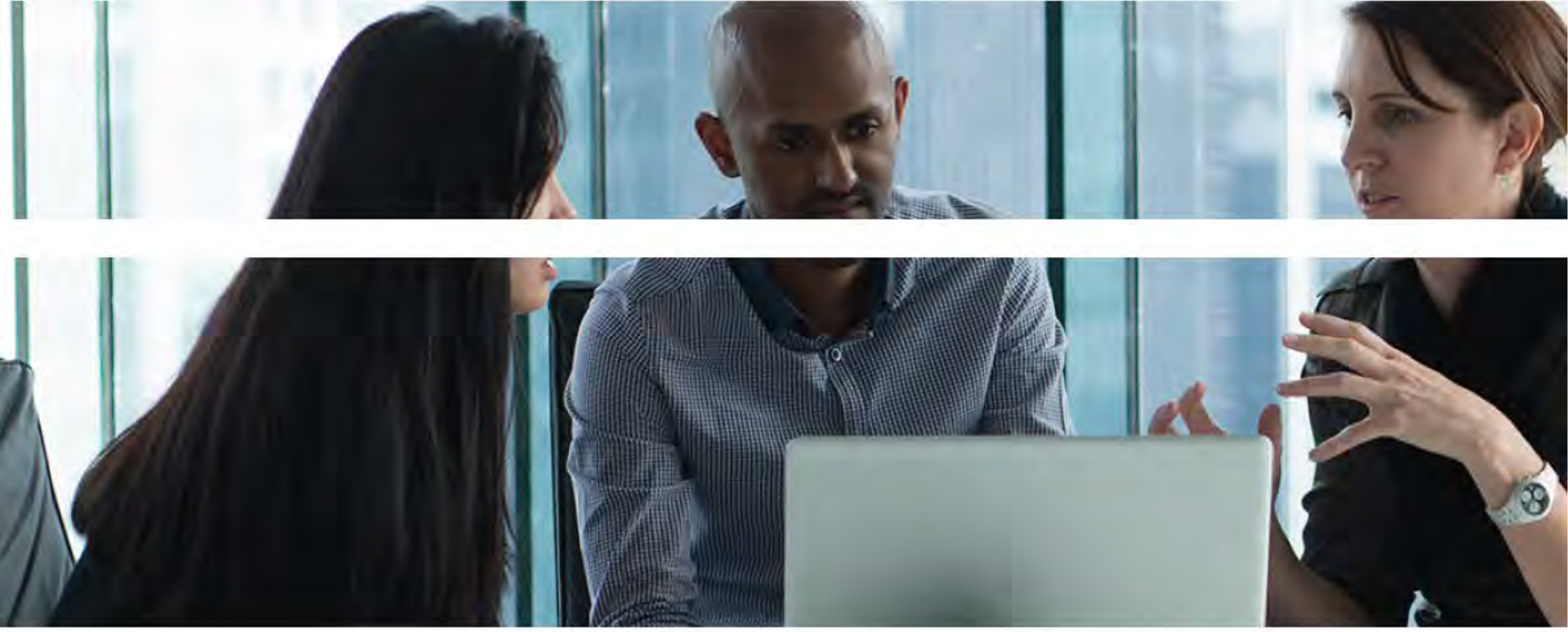
How satisfied are banks with their surveillance solutions?

Participants to our survey stated that their vendor solutions had improved in the period since 2016. 80% of participants believed that their trade surveillance solution had improved, 60% that their eComms solution had improved, and 82% that their voice surveillance solution had improved. Participants noted improvements to coverage, functionality and to alert logic. In contrast, there continue to be concerns over the high volumes of false positives.

When participants were then asked how satisfied they were with their current solutions, as opposed to simply whether or not they felt their solutions, either pre-existing or new, had improved, a very different picture emerged. Only 50% of participants were satisfied with their trade surveillance solution, 45% with their eComms solution and 40% with their voice solution.

Figure 6: Surveillance improvement since 2016 and satisfaction with current solutions





The size of the investments made and satisfaction levels to date demonstrate the sheer scale of the task. Closer examination of the responses reveals that not a single bank was satisfied will all three surveillance channels, although a little over a quarter (29%) were satisfied with two of their channels.

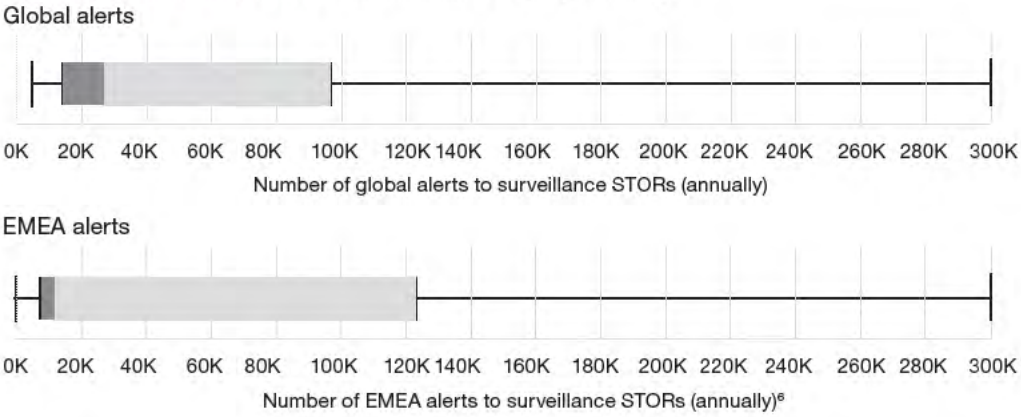
The figures suggest that while real improvements have been made since 2016, further advances are required as regulatory expectations increase and banks move from implementing the basics of surveillance to more complex requirements. Part of the ongoing challenge is undoubtedly to break the current equation of additional surveillance translating to greater volumes of alerts, greater volumes of false positives and increased surveillance costs.

Reviewing surveillance alerts – Is there a need for a paradigm shift?

This box and whisker plot shows the extremities of the alert to STOR ratios. Both for EMEA and globally the majority of the participants are located toward the lower end of the scale with a following tail.

Overall, in EMEA there has been one STOR (or local equivalent) generated every 12,000 alerts and globally the ratio rises further to one every 29,000[5].

Figure 7: Number of alerts per surveillance STOR[4] (annually)



[4] STOR or local equivalent.

[5] Calculated based on STORs (or local equivalent) raised through surveillance activities only for the 17 participants who provided alert and STOR information.

[6] 13 participants plotted for Global ratios and 15 participants plotted for EMEA ratios. Ratios are capped at 300,000 alerts per STOR.

“

40m – Alerts generated by 17 participant banks in the last 12 months

“

Less than 0.01% of EMEA alerts lead to a STOR

Our survey results bring to life just how challenging performing effective surveillance is, and how onerous the task of doing so is becoming. Over the last 12 months, 17 of the banks participating in the survey, have raised a combined global total of over 40 million trade and eComms alerts.

These alerts are raised by surveillance systems tuned to trigger based on certain characteristics of market abuse potentially being present. Every single alert is currently reviewed.

If we drill into the EMEA results for the 17 banks in a little more detail, then we see that 11 million alerts are generated annually. At the end of the review process, less than 0.01% of these alerts are submitted as a STOR (suspicious transaction and order report). In other words, one STOR is generated for every 12,000 raised alerts[7]. Irrespective of whether one believes the number of STORs raised to be either too high or low, a false positive population of 99.99% is an extraordinary statistic. A huge amount of effort is being expended reviewing benign trading behaviour. It does raise the question as to whether it is time for the alerts generation and review process to undergo a paradigm shift.

With continued evolutions in technology, is there an opportunity for the banks to take advantage of predictive modelling and machine learning techniques, and for surveillance functions to risk score both trader behaviour and the alerts themselves to identify higher risk alerts? Rather than review all alerts, could surveillance functions just focus on a markedly reduced population of higher risk alerts? A logical consequence of this would be that more time could be spent undertaking more detailed investigations of the higher risk alert population.

Would this support the generation of more effective outcomes? In part it depends on whether you believe the current ‘alert resolution factories’ can ever effectively investigate millions of alerts. A question for surveillance practitioners and regulators is whether they are ready for a shift away from the perceived imperative of reviewing all alerts.

[7] Calculated based on STORs raised through surveillance activities and excluding those raised through the front office.

Part 3 – Perspectives on the future of surveillance

To what extent does surveillance remain a work in progress?

The industry has made a lot of progress with surveillance, but there is more to do. We asked participants how they would describe the state of their surveillance; in remediation, implementation or business as usual (BAU). The results were surprising. The venn diagram shows the complexity of the answers we received with four banks considering themselves to be operating in all three states, and nine banks considering themselves to be operating in two of the three states. A further two banks have said they are in a state of transformation. Tellingly, not a single bank considers themselves to be operating solely in a BAU state. This question response, perhaps more than any other across the survey, reveals the extent to which surveillance remains a work in progress.

Figure 8: State of surveillance operations across all channels

When asked if their surveillance was in a state of implementation, remediation or BAU, participants responded that their surveillance often operates across a combination of states depending on channel and coverage.

State of surveillance

Implementation Remediation Business as usual (BAU)

> 86% of participants reported strong or moderate appetite for continued investment

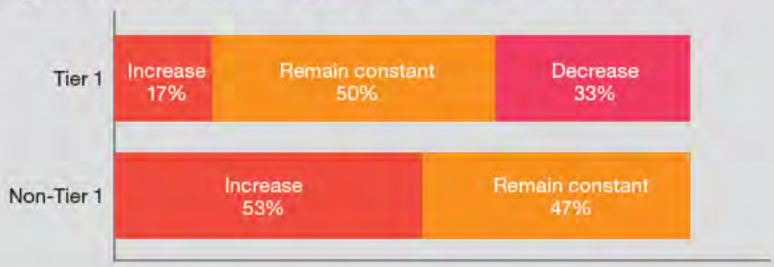
The statistic acknowledges the new norm that surveillance is a journey rather than a fixed point destination. There will always be more work to be done, and no cause for complacency. The message that there is further work to be done evidently resonates as 86% of participants reported that there was either a strong (19%) or moderate (67%) appetite for continued investment. This is despite the fact that the participants[8] (15 of the 21) have spent almost three quarters of a billion dollars on surveillance over the last two years. Over the next 12 to 18 months, our participants predicted that they will spend a further total of $363 million[9].

Figure 9: Planned investment spend for the next 12-18 months

> $363m – Predicted spend on surveillance over the next 12 to 18 months[9].

Predicted future levels of investment point to the fact that participants continue to place their faith in technology. On average Tier 1 banks will invest four times as much as the non-Tier 1 banks. However it is interesting that the investment patterns of the banks differ, with the non-Tier 1 banks much more likely to seek to increase headcount while the Tier 1 banks appear to now be at a point in the cycle where they can contemplate driving efficiency and reducing headcount (33% estimating a decrease in headcount).

Figure 10: Anticipated changes to surveillance headcount



While the rate of investment is now starting to diminish, it remains considerable and the subject clearly still resonates at C-suite level. As the impact of further investment is made it will be interesting to observe the extent to which sentiment changes and more banks believe themselves to be entering a state of BAU.

[8] Of the 21 participating banks 15 provided data on historical spend. Values were converted from local currency to USD using Bank of England exchange rates on 19 February 2019.

[9] Of the 21 participating banks 15 provided predicted CAPEX spend and 15 provided predicted OPEX spend. Values were converted from local currency to USD using Bank of England exchange rates on 19 February 2019.

What are the priorities over the next 12-18 months?

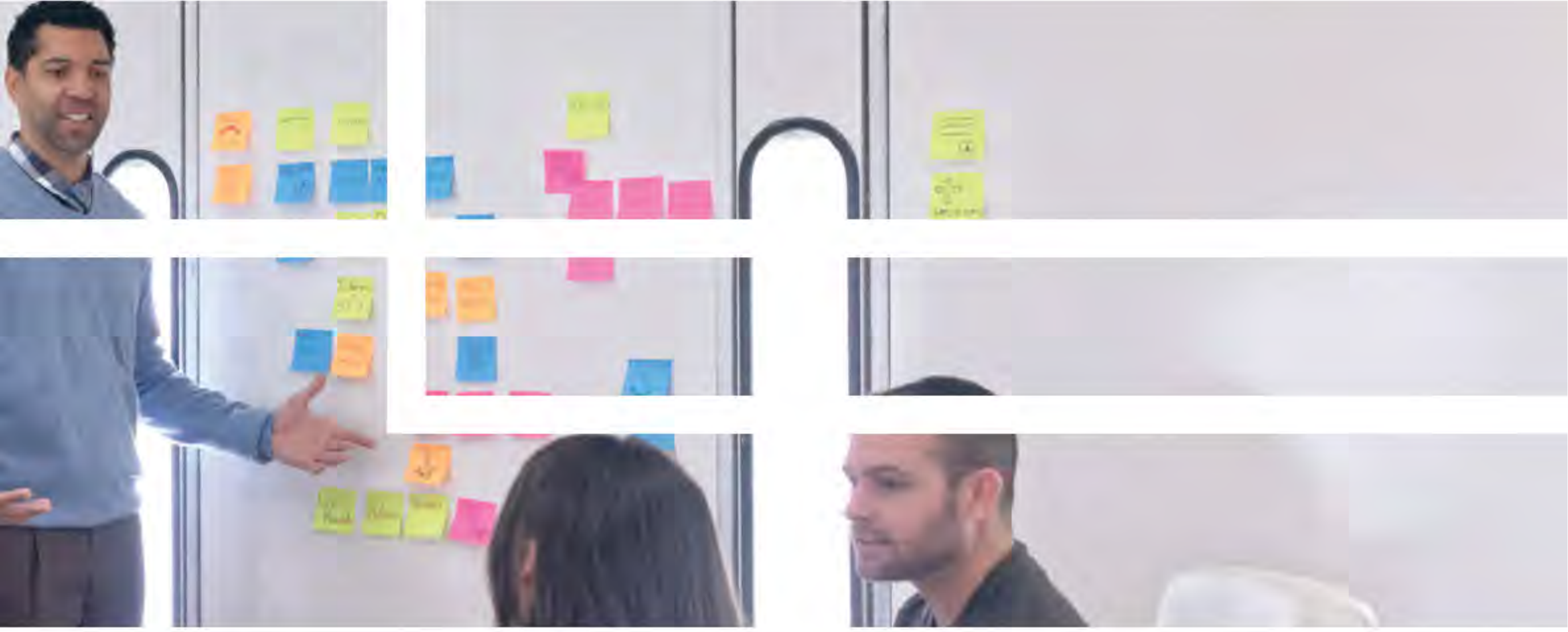
A key focus for the next 12-18 months across all participants is continuing with implementation programmes and seeking to better leverage existing investments. This is a core activity for all participants and reflects the endeavours to move to BAU.

Beyond this there remains appetite to embrace new technologies, reflecting the symbiotic relationship between the banks and the software vendors. Early adopters are enthusiastic about piloting and deploying new technology or the application of new analytical techniques, and where these are successful the early majority follow.

There is currently a buzz around both voice surveillance and application of trader profiling and machine learning techniques. In particular, it would appear that transcription technology is finding its voice. The 2016 survey identified, that aside from three early adopters, firms were hesitant about investing in automated voice surveillance due to concerns over accuracy rates. That sentiment has definitively changed and there has been an increase in interest in implementing voice technology with eight implementations since 2016. This has been driven in part by regulation and also by a sense that voice presents a relatively high unmitigated surveillance risk at present. While it is too early to predict the success of voice transcription for surveillance, there is a sense from participants that the technology is maturing and that transcription accuracy rates are improving and reaching the required baseline. Certainly a critical mass of participants are now using or currently implementing voice technology, applying both phonetic and transcription techniques. A number of participants have plans to select and implement voice surveillance over the next 12-18 months. It is clear that the direction of travel is for enhanced voice coverage.

Machine learning and AI are widely viewed as the 'next big thing' to increase the effectiveness of trade surveillance. A small number of participants use vendor software that applies behavioural profiling techniques, but as yet bespoke approaches, including predictive modelling are at best in their infancy. However, if participants make the progress that they hope to, then within a two year time frame there will be widespread adoption of these techniques.

The pace of technological change is unrelenting and banks are increasingly keen to embrace technology where it provides a material uplift in their ability to potentially detect market abuse. Analysing participants' adoption intentions suggests that the capability gap between early adopters and the late majority and laggards is going to continue to grow.



How confident is the industry about the future of surveillance?

In our opinion the surveillance industry has come a long way since 2016. Vendor solutions have evolved to provide more coverage, superior alert logic and more intelligent means of identifying market abuse. Surveillance practices have transformed, and the surveillance coverage over employees has exponentially increased with orders, executed trades, internal and external eComms over a host of chat platforms, and now voice communication all monitored on a T+1 basis. Surveillance has never before been so all encompassing. Surveillance gaps remain but they are acknowledged and the industry is working to address them.

Therefore the industry can have justifiable confidence that layers of detective controls are now in place, increasing the likelihood that a market abusive event would be found. The investment in surveillance sends a clear message that the industry is committed to the detection and prevention of market abuse. This in of itself must act as a deterrent to traders contemplating misconduct.

This is borne out by the positive sentiment emanating from the participants. A majority are optimistic about the ability of surveillance to keep pace with the changing nature of risk, and changes in trading practices. We have also seen there is a growing belief that integrated surveillance with its ability to triangulate signals across channels is on the horizon.

While no one can dispute that achieving effective surveillance and keeping pace with regulatory expectations is challenging, and is likely to remain so, the surveillance industry enters 2019 in robust shape, with firm foundations set for safeguarding against the risk of market abuse.

About this report

We interviewed 21 banks; 14 of which also participated in the 2016 survey, allowing us to draw out a view of how the organisations have evolved. While we have focused on ‘Markets’ business within the banks, which as a sub-sector are the furthest ahead and give us the best view of ‘leading practice’, our intention was to provide a representative view across organisations of different size: six participants could be described as being Tier 1 with the remaining 15 representing banks of various sizes with different international footprints.

We gathered responses to 93 questions during face-to-face interviews with representatives of the participant banks (typically Heads of Surveillance). Gathering information in this way gave us an opportunity to probe responses and elicit the richest detail on how each bank is tackling challenges with the effectiveness of surveillance. After the interview, participants were given the opportunity to validate the numeric responses we had captured to confirm we had an accurate data set for our analysis.

Non-numerical participant responses were varied in length and structure, and have been subject to a level of standardisation in order to place them within derived categories to enable comparison.

Contacts

Graham Ure
Surveillance data and technology – Partner
M: +44 (0)7889 644672
E: graham.ure@pwc.com

Rukshan Permal
Market abuse regulation – Partner
M: +44 (0)7595 611533
E: rukshan.permal@pwc.com

Anne-Marie Edmonds
Market abuse regulation – Director
M: +44 (0)7808 020659
E: anne-marie.edmonds@pwc.com

Alex West
Market abuse regulation – Director
M: +44 (0)7841 567371
E: alex.e.west@pwc.com

Mark Chopping
Surveillance data and technology – Director
M: +44 (0)7889 645115
E: mark.chopping@pwc.com

pwc.co.uk

190321-151012-JF-OS