November 2020

2025 – The Future of Market Abuse Surveillance

Contents

Foreword 1

January 2020 – A new challenge 2

Covid turmoil, and the aftermath 6

The STOR visit 9

2025 and looking back 10

Building the foundations 12

Projects to deliver incremental improvements across the programme 18

Deploying behavioural analytics 22

Reflections from the summit 27

Foreword

Dear readers

In the four years since our first Market Abuse Surveillance Survey in 2016, surveillance practices across the industry have transformed. Surveillance coverage over employees has exponentially increased with orders, executed trades, internal and external comms covering a host of chat platforms and voice communication all monitored. Surveillance is more comprehensive and more technologically advanced than ever before.

To understand the future we must have a clear view of the present. Surveillance advancements have been driven by the investments made by financial institutions and through their symbiotic relationships with the software industry who have provided the technological advancements necessary to deliver more effective surveillance. However, downward pressure on budgets is commonplace, and not always congruent with the need to address continued gaps in surveillance coverage, enduring challenges with data and a desire to pursue relentless improvement. Additionally, the continued avalanche of false positives and their undiminished volumes, are an impediment to attaining productivity gains and the corresponding cost efficiencies.

In this environment we are seeing new market abuse risks emerge. The ways in which we are working are changing, driven by the Covid pandemic, and will continue to require corresponding adjustments in how surveillance is performed. At the same time regulatory scrutiny continues unabated, driven by the imperative of ensuring orderly and clean markets.

Any prediction of the future is fraught with peril. Nonetheless we believe that surveillance advancements will principally be driven by technology, and yet technology progress is typically over-estimated over two years but under-estimated over ten years. While acknowledging the difficulties of peering too far into the future, this publication presents a fictionalised account of a Head of Surveillance looking back on the challenges they faced, here and now in the present, and reflecting on the steps taken in initiating and delivering on a successful surveillance transformation programme through to 2025. In doing so our Head of Surveillance contends with Covid, STOR visits, organisational restructures and addressing the difficulties inherent in achieving effective surveillance.

While we have consciously chosen to present a fictional account, we have sought to provide a bold yet realistic vision as to how surveillance could evolve over the next five years. We hope that this publication will prove an engaging read, and will contribute to shaping the future of surveillance.

> “Any prediction of the future is fraught with peril. Nonetheless we believe that surveillance advancements will principally be driven by technology, and yet technology progress is typically over-estimated over two years but under-estimated over ten years.

January 2020 – A new challenge

"There's nothing to see here, we are '*best in class*'" was the ringing endorsement I took from my first meeting with the outgoing Head of Surveillance. Coming from an experienced and respected industry leader, this gave me some comfort that I would have a little bit of 'time' to settle into my new role.

In January 2020, I took the position as Head of Surveillance at an international bank headquartered in London. I had extensive experience in surveillance from my previous roles, having overseen trade surveillance for another bank for the past four years. I was a respected surveillance professional and had been the deputy head for a while, but I had never had the 'top job' and never had a role overseeing the full breadth of surveillance activities across a bank, nor been responsible for budget requests, the global operating model or the overall future roadmap. Walking into my new office just after the start of the New Year, I was genuinely excited about what lay ahead and had high hopes and expectations as to what I would achieve in 2020.

Although my predecessor painted a rosy picture of the environment, it was made clear to me during the interview process that, although much progress had been made, further enhancement could still be achieved through a well funded multi-year programme. My impression before joining the bank was that it was lagging behind peers in a number of areas and the results of a PwC Market Abuse Surveillance survey which I reviewed on my first day in the job made that conclusion inescapable. While the bank wasn't one of the biggest surveillance spenders, there was an internal perception that costs were disproportionate to risk. On my first day in the office, the Global Head of Compliance joked that I had one very simple objective: "Better surveillance, lower cost".

January presented me with a great opportunity to get into the detail of the existing surveillance framework. I read hundreds of pages of process documentation; I met each of my team leads at least twice, I listened to every team update, I met with each of my stakeholders across Compliance and those leading the business, and I spent three days in each of our off-shore locations.

By the end of the month, it was clear to me that we had challenges, more than the bank had let on about and probably more than they realised themselves. The messages coming back to me from my stakeholder interactions were, mixed at best, downright critical at worst. Some I had expected – no Monitoring and Surveillance function could say they were perfect – but others kept me awake at night and it was clear to me that we were certainly not '*best in class*'.

To add another layer of challenge, the FCA had informed us that they intended to carry out a STOR visit just before Easter. The time I thought I had to settle in had quickly evaporated and reality had kicked in. The future planning and the longer term enhancement projects would have to wait. I needed to focus on fire fighting and work out exactly where we were ahead of the imminent STOR visit.

> "
>
> On my first day in the office, the Global Head of Compliance joked that I had one very simple objective: "Better surveillance, lower cost.

My initial findings were largely as expected, but still presented one or two surprises: our existing e-comms solution, which had been in place for almost a decade, was fully lexicon based and generated an average of 55,000 alerts a month. Although initially running on trader communications only, it had been extended over recent years to cover all front line employees, utilising the same lexicon terms for all. The programme was 'noisy' and created very few 'qualified' alerts being escalated for action. On top of that, we had a backlog of e-comms alerts. This had resulted from a system failure in early 2019 which led to a week's worth of Bloomberg chats not being ingested. Once processed some months later, they created over 25,000 additional alerts that the team hadn't had the capacity to clear. Worse still, an Internal Audit report published in December 2019 had concluded that the lexicon itself wasn't 'fit for purpose', without specifying enhancements required. Nothing had been done to address Internal Audit's findings before I arrived as the CCO took the view that I would be best placed to determine the actions required.

On a more positive note, our core trade surveillance solutions were solid from a technology perspective. We used one platform for exchange traded products and my predecessor had secured a budget in 2018 for a new solution to cover other venues and OTC activity, but I gathered the implementation hadn't been smooth and that the solution wasn't fully operational. Fixed Income coverage was poor and we had no models focused on cross-product or cross-market related risks, which gave me cause for concern in the context of the FCA's Market Watch 56. Data quality challenges had never been fully resolved. Some models generated excessive alert volumes and others, suspiciously, generated none. The basis of model calibrations weren't well documented and the model validation process didn't seem to answer the exam question of whether the models actually mitigated the risk.

Voice surveillance was entirely manual and sample sizes were low. I was comfortable that I could argue a good risk-based rationale for the approach, but the review was time consuming and I resolved to explore automation at the earliest opportunity. While it remained widely accepted that voice surveillance technology was still evolving, and we were likely to be comparable with our peers, I had a nagging sense of discomfort over the current approach given the scale of our high-touch trading and the low level of detective control exercise over it.

Taking the different surveillance channels together, our coverage assessment highlighted gaps against high risk market abuse types and a consultant's report about the quality of our risk assessment called out deficiencies in our approach. I knew a good quality risk assessment was a fundamental baseline for robust risk-focused surveillance but I also didn't want to distract the team with a lengthy risk assessment process at this point and lose sight of the more pressing issues at hand. There were technology and process enhancement projects in flight and although I could not offer much time to support in the short-term, I thought it was appropriate to allow the project teams to continue to progress their work. I believed we could continue to implement and embed these new capabilities in parallel with forming a better understanding of areas of risk.

There were also a number of legacy manual controls in operation which had been designed to fill gaps in coverage and to address previous Internal Audit findings. There was a strategy to move as many of these across to automated solutions and we worked with our technology colleagues to create an annual 'book of work' once our change stream budgets were agreed each year.

Despite the challenges I had initially identified, after a few weeks in the role, I was reassured that I had a good team. We had a strong core team of surveillance SMEs, supported by a small number of ex-traders in London, New York and Singapore and technologists who understood the challenges and shared a vision of a better future for surveillance.

I wanted to make some changes, in particular to bring in more experienced hands to lead on more complex investigations and to support our junior off-shore team members who didn't have the experience to interpret some of the signals coming through the data, yet who we were heavily relying on to close alerts. This issue seemed to result from a strategy of rapidly building up large teams in our offshore locations through the preceding couple of years and having created the structure and initially recruited and trained well, these teams had suffered with high rates of attrition as other organisations set up similar operations in the regions and enticed them away through greater financial incentives.

We had also been subject to the automation boom and seen a number of attempts to launch RPA robots across the programme. These were built to try and automate some of the existing manual controls ahead of making full technology changes, but were primarily deployed to attempt to reduce costs by replacing headcount. There had been limited success in deploying bots in a stable manner and in most cases, the team had reverted to the original way of doing things. Although we adopted a federated approach and trained our team members to build the bots themselves, the positives achieved in increasing their skills while trying to find new ways of working, did not seem to dispel the clear scepticism surrounding the project.

Nobody had said that the step up to Head of Surveillance would be easy and my first 30 days had been a whirlwind of frenetic activity as I took stock of current capabilities and identified the areas for improvement. I now had some sense of where the proverbial skeletons were hiding. My abiding nervousness, if not fear, was that I did not have time to create a credible roadmap for a stronger surveillance framework before the forthcoming FCA STOR visit. Over and over I played out in my mind the questions I least wanted to be asked, mentally rehearsing the answers, and agonising over the FCA's prospective reaction to them. In the dark hours of the night the FCA Market Oversight team were my demons.

> “
> Nobody had said that the step up to Head of Surveillance would be easy and my first 30 days had been a whirlwind of frenetic activity as I took stock of current capabilities and identified the areas for improvement.

> “My impression before joining the bank was that it was lagging behind peers in a number of areas and the results of a PwC Market Abuse Surveillance survey which I reviewed on my first day in the job made that conclusion inescapable.

Covid turmoil, and the aftermath

Immersed in the intensity of the new role, I'd scarcely noticed the news reports of a virus in China. And then, suddenly Covid-19 and Lockdown were upon us, and I had a whole new set of concerns.

After the initial seismic shock of Lockdown, the abrupt end to the daily commute and the start of back to back video conferencing, I came to terms with the new way of working. The bank's infrastructure was superb and the transition to having my whole team working from home was smoother than I could have imagined.

Thankfully, I didn't personally catch the virus although several people in my team did at various points and a few had a very tough time of it. We did our best to support those individuals and help them safely return to work which is one of the things I am most proud of. Even those of us who didn't get ill felt the mental health effects of prolonged social distancing but we worked hard to maintain the team ethos and to be supportive of each other. This was aided by the tone from the 'top' and the strength of our existing culture.

Although we were well advanced in providing the FCA with the requested documentation for the planned visit and we had held a number of initial calls on the topic, the effect of the pandemic had required them to delay the STOR visit until things became clearer.

Any sense of respite was short-lived however. March and April count as one of the most challenging periods of my career. Automated trade surveillance in particular buckled under the strain of the huge increase in trade and order flows as the global economy reacted to the scale of the pandemic and investors sought sanctuary from plunging markets. At one point alert levels touched six times the usual daily levels. Email surveillance was not far behind as the alerts often exceeded 5,000 per day as our revenue generating staff found themselves working remotely, some for the first time in their careers. As alert levels grew out of control, we initially tried to maintain existing working practices and review everything, but this soon proved to be impractical and we needed to apply some sampling methodology to cope. We also chose to completely disable some of the coverage relating to areas our assessment had determined to be of lower risk.

In volatile markets there was no opportunity to recalibrate surveillance models due to the resource constraints, current ponderous IT processes and the inflexibility of our model governance process, which meant we had no option but to retain existing parameter settings. Even if we could have changed them, where would we have set parameters to be meaningful?

The team pulled together really well and by June our processes and operating rhythm had switched over to the 'new normal'. The bank also communicated that no one should expect to be back in the office full time until January 2021 at the earliest. It became clear towards the end of the summer that a longer term shift in working practices was inevitable and that surveillance needed to adapt as a consequence.

By the end of the summer things had settled down and we were back to running our full suite of controls. There was a fairly painful exercise to retrospectively document some of the operational decisions we'd made at the start of Lockdown but experience told me that the effort would pay dividends in the future should the FCA ask us to set out how we'd responded to changing risk profiles during 2020.

The FCA did not disappoint in this regard. At the end of August, they confirmed that they wanted to revisit the scheduling of the STOR visit and that it would take the form of a virtual visit in October.

In the early autumn, we held a series of virtual workshops with the business to explore how Covid had changed our risk profile. As well as implementing additional remote supervisory processes we increased the coverage of staff subject to e-comms monitoring to capture some of the core employee roles and for the first time to add Compliance staff into scope.

Regulators had expressed concerns in papers and speeches about flows of sensitive information which led us to include anyone that was likely to come into contact with UPSI. In addition to the Compliance Control Room, this extended to 'pitch' support staff, transactional legal, marketing and even those in the print room! We also supported core Compliance to develop additional guidance about use of personal devices and how to keep sensitive information secure in a home working setting, an exercise that allowed us to build stronger relations with our colleagues, some of whom had been critical of the value of surveillance.

We also reviewed our e-comms lexicon. I engaged with the internal auditor who had critiqued our approach in 2019, and the key feedback was that the existing list of terms had not been updated since the system was first introduced. The lexicon consisted of just under 1,000 terms, so we decided that the most efficient way to review it was by commissioning a contractor to accelerate the process. With this work underway, I was further staggered to hear from my e-comms lead that the reason the lexicon was not amended regularly was because it was not owned by Surveillance. It was created by the Advisory Compliance team, who had in the past agreed its content with the Business Risk Management teams. Surveillance did not even get a seat at the table and even now could only make suggestions that would be taken away for consideration.

So it transpired that more than half of my resources were reviewing alerts from a programme they had little or no involvement in determining; a programme that generated over 99.5% false positives, which in turn received a lot of Senior Management attention and anecdotal criticism; and where we had picked up a number of Internal Audit findings that we were almost powerless to resolve by ourselves. This needed to change.

Ironically, before I joined it had been decided that an upgraded e-comms surveillance programme should be implemented. The view was that this would resolve the apparent lack of effectiveness and efficiency in the current solution. From what I was seeing, we needed to fix some internal issues first before investing in a new solution. However, funding was already approved and the project team assembled to start the initiative, so I needed to move quickly to address the restrictions the current approach was creating. I took this opportunity to demonstrate how I and the surveillance team could make a real difference.

> "
>
> Regulators had expressed concerns in papers and speeches about flows of sensitive information which led us to include anyone that was likely to come into contact with UPSI. In addition to the Compliance Control Room, this extended to 'pitch' support staff, transactional legal, marketing and even those in the print room!

I started to design an innovative approach to e-comms surveillance that would both address our current issues as well as greatly improve its effectiveness. However, my first foray into the world of technology budgeting quickly suppressed my enthusiasm. One of the biggest challenges I had to tackle that arose out of Covid was the pressure put on budgets. Cost pressure had been there from day one, but tougher market conditions in 2020 led to further evaluation of costs and an even tighter process around budgets for longer term investment. It was announced that current year spending would cease for all but regulatory committed development work and that the following year's budget would be reduced by 25% immediately and 2022 would see a 20% cut. These reductions would not only apply to new initiatives, but also the current ones and therefore we would need to quickly reassess our areas for priority and consider revised timelines for delivery.

Adapting our resource mix and creating greater efficiency through the use of technology had always been in the plan, but 2020 made that need far more acute. Our new e-comms solution business case was focused on the reduction in alert volumes it would deliver and the consequent reduction in headcount in our offshore centres. In reducing the budgets, this would directly limit what we could achieve.

It was quickly becoming clear that a more innovative approach was going to be required if we were going to be able to introduce the significant changes we needed in order to raise the capabilities of the team and to keep us on par with both our peers and the expectations of regulators.

My prepared script for the FCA visit detailing our significant upcoming technology upgrades was going to have to be tempered somewhat.

“

Cost pressure had been there from day one, but tougher market conditions in 2020 led to further evaluation of costs and an even tighter process around budgets for longer term investment.

The STOR visit

Then finally the ‘virtual’ STOR visit took place and in some respects it was an anti-climax, and there were no demons on the day. Reflecting upon it, the visit was analogous to an exam. We’d done the preparation and our revision had been thorough; but there were questions we were better and worse prepared for. No amount of verbal eloquence is a substitute for presentation of facts, or in our case presentation of the evidence of full compliance with MAR. I had an anxious wait for the results, and then on a cold, wet November morning the FCA response duly arrived.

My eyes raced down the text, skim reading past the opening pleasantries – “Having taken the time to reflect upon the information you provided us with, as well as our interactions with you during the visit, we now offer you our feedback.” There was no doubting the thoroughness of the review and the dissection of surveillance in the bank.

There was credit for the areas where robust surveillance and controls were in place, but the letter moved quickly to an articulation of the identified gaps in the bank’s surveillance programme and expressed concern over the apparent lack of urgency in the addressing of them.

I was not surprised by the concerns expressed over our continued gaps in Fixed Income coverage and our limited coverage of surveillance over orders, and to a lesser degree by the observation that there was a lack of clear lineage between the risk assessment and the surveillance models deployed, and that further transparency of this was required. The FCA also expressed concern over the lack of effective cross-market cross-product manipulation surveillance and the need for tactical controls to mitigate this risk.

While I acknowledged these points I felt the statement that the overall surveillance programme lacked coherence and specificity was harsh, especially given my own relatively short tenure in the role. Shaping a three year Surveillance programme and associated budget had been front of mind before Covid arrived and necessitated an immediate focus on the day to day business of running the operation.

The virtual visit was certainly thorough, and I did wonder whether it was more exacting than a face to face visit would have been within the pre-Covid environment, as I received unexpected challenge around the quality assurance over the alert review process, and the depth and breadth of the procedures we had in place to support alert review.

To a large degree I could have predicted the content of the letter if not the tone, but there were two areas of FCA focus that I had simply not anticipated, although upon reflection the clues had been present in recent communications from the FCA.

The first was a desire for the bank to undertake some form of thematic analysis or retrospective review to ensure that new risk dynamics arising from Covid were captured in our risk assessment and that calibration of our models during the period of heightened market volatility had been appropriately considered. The measures we had taken to document our actions earlier in the year took us some way towards addressing this, but we had not actually undertaken the lookback reviews that the FCA were now requesting.

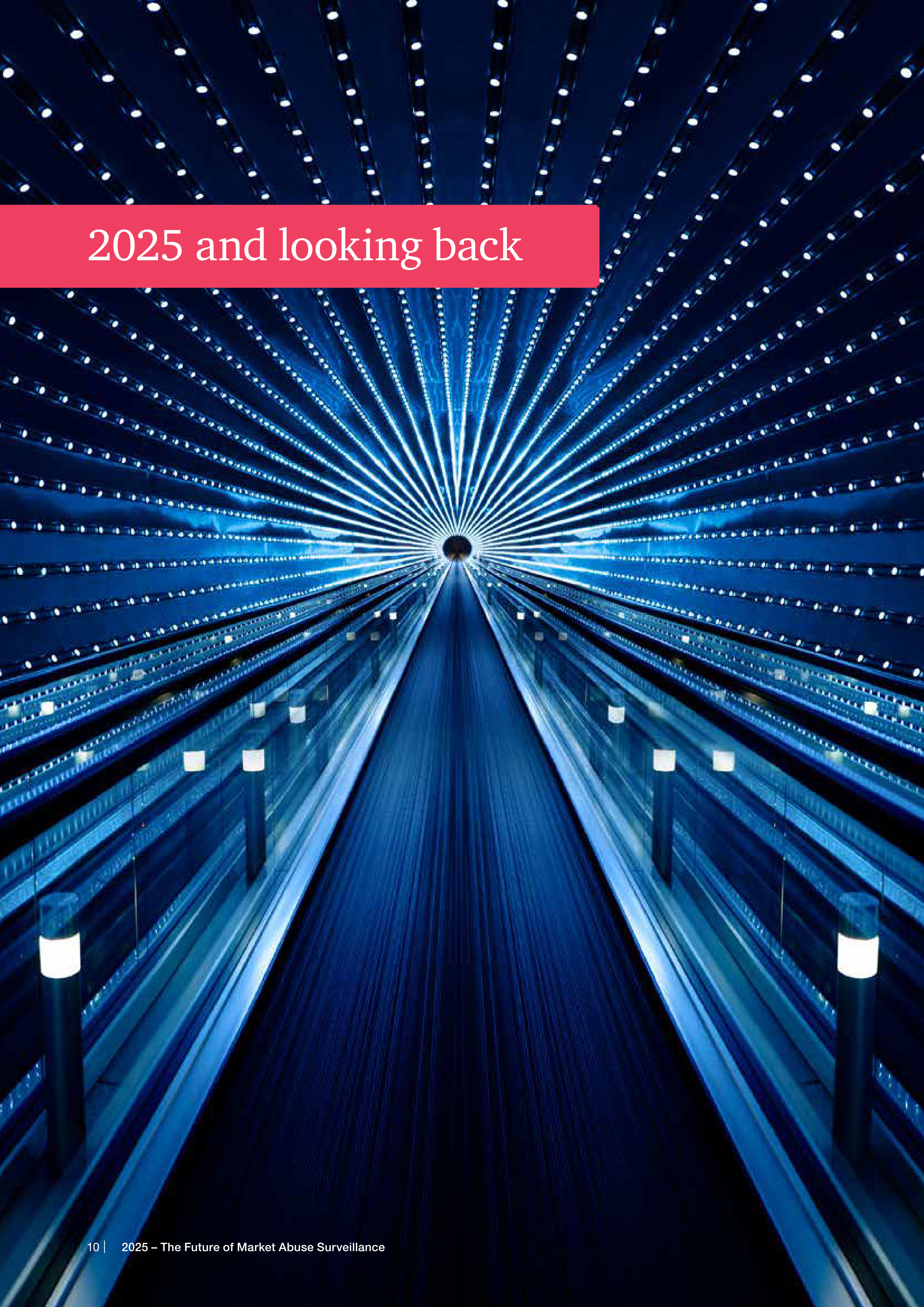
The second was to examine the effectiveness of our a-comms surveillance and to ensure that our approach was proportionate to the level of potential risk arising from both monitored and potentially unmonitored voice communication and to ensure controls were appropriate.

I reread the letter several times, and reluctantly embraced the inescapable conclusion that my metaphorical exam paper had just marked C-. There was a lot to do, starting with the sharing of the outcome of the STOR visit with the Global Head of Compliance.

They say every cloud has a silver lining. The STOR visit was the unwelcome end to what had been, on a myriad of levels, a difficult and personally challenging 2020. But as the New Year was ushered in, bereft of crowds and firework displays, I recognised that the STOR visit was not a catastrophe, but rather an opportunity and while it was not exactly the outcome I would have wished for, for the most part the findings had resonated with my own views as to the current state of the surveillance function and my underlying beliefs as to where improvements needed to be made.

The words and tone of the FCA’s findings resonated with greater impact within the bank than any words I could have written in support of the need to increase our surveillance capability. The mandate for change was there – what was I going to do with it?

2025 and looking back



As I sit here five years on, reflecting on the hard work, challenges, setbacks and the literal transformation of surveillance within the bank, I can remember my moment of epiphany with crystal clarity.

I knew all the imperfections inherent within seeking to deliver an effective surveillance and monitoring capability, and had lived with those frustrations but that didn't mean I had to accept them. I knew what I wanted to achieve. What if I threw the rule book away? The question was did I have the courage of my conviction to set out my vision, take others on the journey with me and then deliver on it? In a heartbeat I knew the answer, and over the following two to three days set out my plan with a growing sense of excitement.

My business case to the CCO began with the famous quotation from Albert Einstein, "... insanity is doing the same thing over and over again, but expecting different results." I briskly stepped through the current issues, many of them highlighted by the STOR visit and then set out a bold and ambitious plan to create a transformed surveillance function able to provide the detective controls appropriate to support the bank's stated risk appetite. The scale of change would be significant and was planned out over a four year period. I was forthright in stating that we must be steadfast in steering to the course set, not being diverted and that if we had the courage and conviction then the budget would be cost neutral over the period. If the bank would commit to preserving the 2020 levels of surveillance budget for each of the next four years then I would oversee the delivery of the desired transformation in our capability. I got the budget commitment and the rest as they say is history. So what changed over the five years? Arguably everything; at least at some level. The strategic blueprint and roadmap set the tone for a different kind of surveillance.

The blueprint set out three stages of progressive capability development within a ten-point plan that became known amongst the team as the ten commandments:

Building the foundations

1. Building data partnerships within the organisation

2. Understanding, collating and fixing the data and architecting the solution

3. Setting up the governance and operating model for success

Projects to deliver incremental improvements across the programme

4. Implementing a cloud based computing strategy

5. Consolidated case management and effective MI

6. Delivering cost effective outcomes based comms surveillance

7. Harnessing RPA

Deploying behavioural analytics

8. Development of a behavioural analytics capability

9. Understanding risk and dynamically responding to it

10. Delivering on conduct surveillance

It would be disingenuous to state implementing this was easy or that we always travelled in a straight line, and of course we had the odd false start and wrong turn. But at every turn I encouraged my leadership team to challenge conventional wisdom and the orthodoxy of how things were done today. I can sit here today and confidently assert that the investments made, particularly in technology have enabled a transformative capability which is now 'best in class' or very close to it. Vexing challenges such as surveilling for cross-product and cross-market manipulation or increasing my ratio of alerts generated to alerts of interest, that were close to intractable in 2020 are now firmly in the rear view mirror. That said the risk landscape is constantly changing and we have no shortage of new challenges to traverse.

Building the foundations

Building data partnerships within the organisation and architecting the solution

I had a clear vision. Our surveillance would be informed by a complete and good quality data-set designed and then consolidated to support our requirements. That data would then feed into a vendor ecosystem of solutions supported by an in-house and custom built analytics layer. A consolidated case management system capable of triaging alerts would give us detailed and timely MI available at our fingertips. Easy to articulate but far from simple to deliver.

I was well aware that the rock upon which most surveillance programmes floundered and perished was data. The 2019 PwC Market Abuse Surveillance survey had noted that “For Heads of Surveillance today it’s a truth universally acknowledged that good data is the key to performing good surveillance.” Before solving issues around data quality I needed to solve the more pressing challenge of data availability and I was determined to build firm foundations. If I could get the data right, I reckoned I’d be halfway to delivering on my Surveillance Programme.

I worked hard to build stakeholder support within the bank, particularly with IT, but also with other functions with whom I could make common cause. I engaged with both the business and HR and built consensus on the need for an ambitious data transformation programme and agreement on the shared objectives, and a willingness to share the overall cost to develop a solution.

As a consequence a programme was initiated, a partnership between the business, HR, Compliance and IT to create a data store that allowed for a consolidated view of breaches and alerts for an individual trader and which ultimately would facilitate the transition to a far more behavioural approach to surveillance.

Investment budgets were pooled, with the objective of creating one data source and analytics capability across all dimensions of conduct.

This proved to be the first of many engagements where multiple internal parties were able to come together to utilise the same technology enhancements across a number of disparate objectives. I was delighted when a three year investment case was agreed with all parties, on the basis of cost efficiencies, common functionality and bespoke outputs that would be delivered on completion

> “
> For Heads of Surveillance today it’s a truth universally acknowledged that good data is the key to performing good surveillance.

Understanding, collating and fixing the data and architecting the solution

Getting the budget to build a Conduct and Compliance-centric data lake was a massive win. But I quickly learnt that it is not as simple as sourcing all the data you can find and throwing it into the lake. Data has always been the key to good quality surveillance and effective misconduct detection. Data is never perfect, but without the existence, accuracy and completeness of relevant data, genuinely insightful analysis is not possible. Our ambition to create trader-centric monitoring necessitated designing and architecting the lake properly and understanding how the relationships between data sources could be used to provide indicators of market abuse or conduct risk.

We ran multiple workshops to determine surveillance requirements and to understand what data we needed to support that surveillance and from where it could be sourced. At a quite fundamental level we had to work backwards from the solution that we wanted to understand what data, in what form, was needed to enable it. Determining what analytics to deploy was arguably when the rubber hit the road though. Considerable thought needed to be given to what we were trying to achieve and what real meaning could be drawn from disparate data sets.

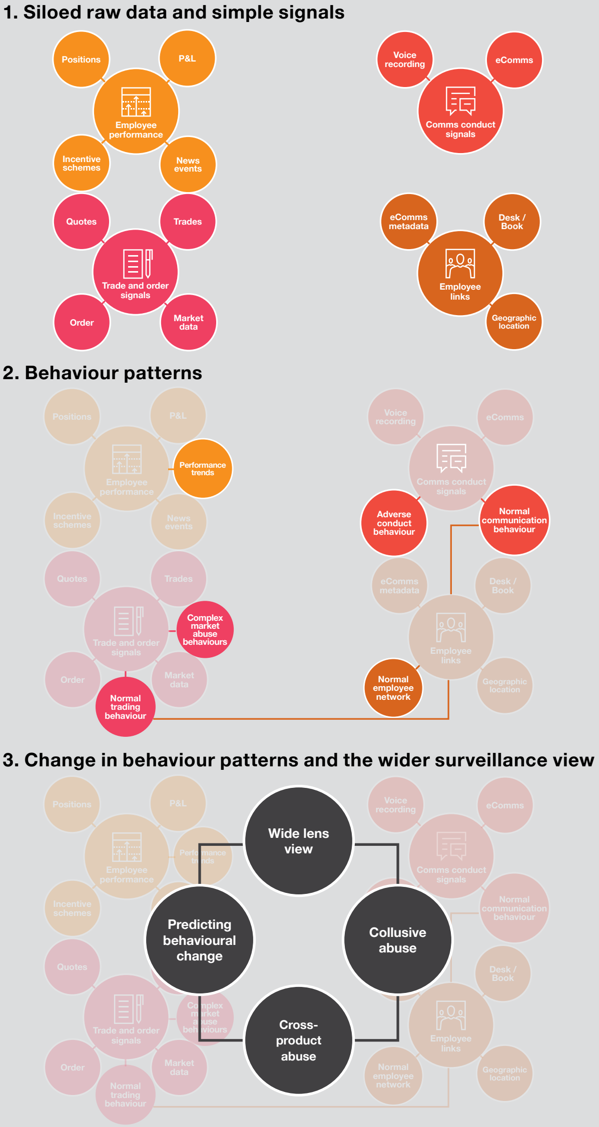
We performed a new market abuse and conduct risk assessment at this stage and for each risk set out in our risk assessment, we analysed potential signals and what analytics could meaningfully be applied with the data available. Once that understanding was in place, we were able to start to determine which analytical techniques were the best fit, and the data required. Our success was in no small part down to the fact that after initial teething issues we worked hand in glove with IT and in particular with their enterprise architect who was able to work to our requirements and accommodate the multiple iterations we went through in refining them.

Our data transformation was hugely ambitious, and we did hit a few bumps in the road. The programme was due to complete at the end of 2023, but a budget reprioritisation that impacted the whole bank meant it didn't actually complete until mid-2024 and we suffered inevitable delays due to data quality and mapping issues. The journey was challenging, but from today's perspective critical to moving towards the next generation of surveillance. Data gaps have now been significantly addressed by upstream technology and process enhancements and the increase in e-trading has simplified some data capture processes as well as improving market transparency.

Fixing your data and architecting your solution

To function effectively surveillance analysts and automated models need many different pieces of data. These pieces of data provide a surveillance and conduct centric view of the world and the data must be prepared and managed with this view in mind. This data is curated in the conduct and compliance centric data lake. The data required for surveillance is often created and stored to support normal business activity and does not consider surveillance requirements. The effort required to ensure the data can support surveillance should not be underestimated. The data needs to be assessed, understood, mapped and standardised across all sources to enable advanced abuse detection functions. The raw input data to the conduct and compliance centric data lake, such as trades, orders and comms, provides the foundation for surveillance, but it is only part of a far wider set of data stored in the lake and used to detect abuse.

Surveillance vendor solutions output signals of interest which are fed back into the lake. This allows layers of increasingly sophisticated behavioural pattern detection to be performed based on these signals, with each layer increasing the richness of data available in the lake. Creating an effective compliance centric data lake requires clarity on how each piece of data will be used and how the varied contextual sources will be linked together seamlessly. The same precision of purpose is also required in considering how the outputs from each layer of analytics can be fed back into the lake to support increasingly sophisticated levels of behavioural surveillance. The conduct and compliance centric data lake – layers of surveillance and conduct centric data supporting the surveillance from raw data to sophisticated behavioural analysis outputs:



1. Siloed raw data and simple signals

2. Behaviour patterns

3. Change in behaviour patterns and the wider surveillance view

Setting up the governance and operating model for success

It was clear to me that a more joined up approach to conduct monitoring and surveillance was required. One of the first areas I sought to tackle in our 2021 roadmap was the governance and organisation model. We had too many organisational silos where conduct monitoring activities were being performed by teams that didn't communicate with each other. Three separate teams (two in Compliance and another in 1LOD supervisory function) generated conduct focused metrics. The Global Control Room (under a Compliance reporting line) monitored for breaches of policies around information barriers, personal account dealing as well as G&E. A separate Compliance team monitored annual policy confirmations, breaches of block leave requirements and training completion. The supervisory function oversaw completion of desk head attestations around trader P&L and risk indicators like cancel/amends and mandate breaches.

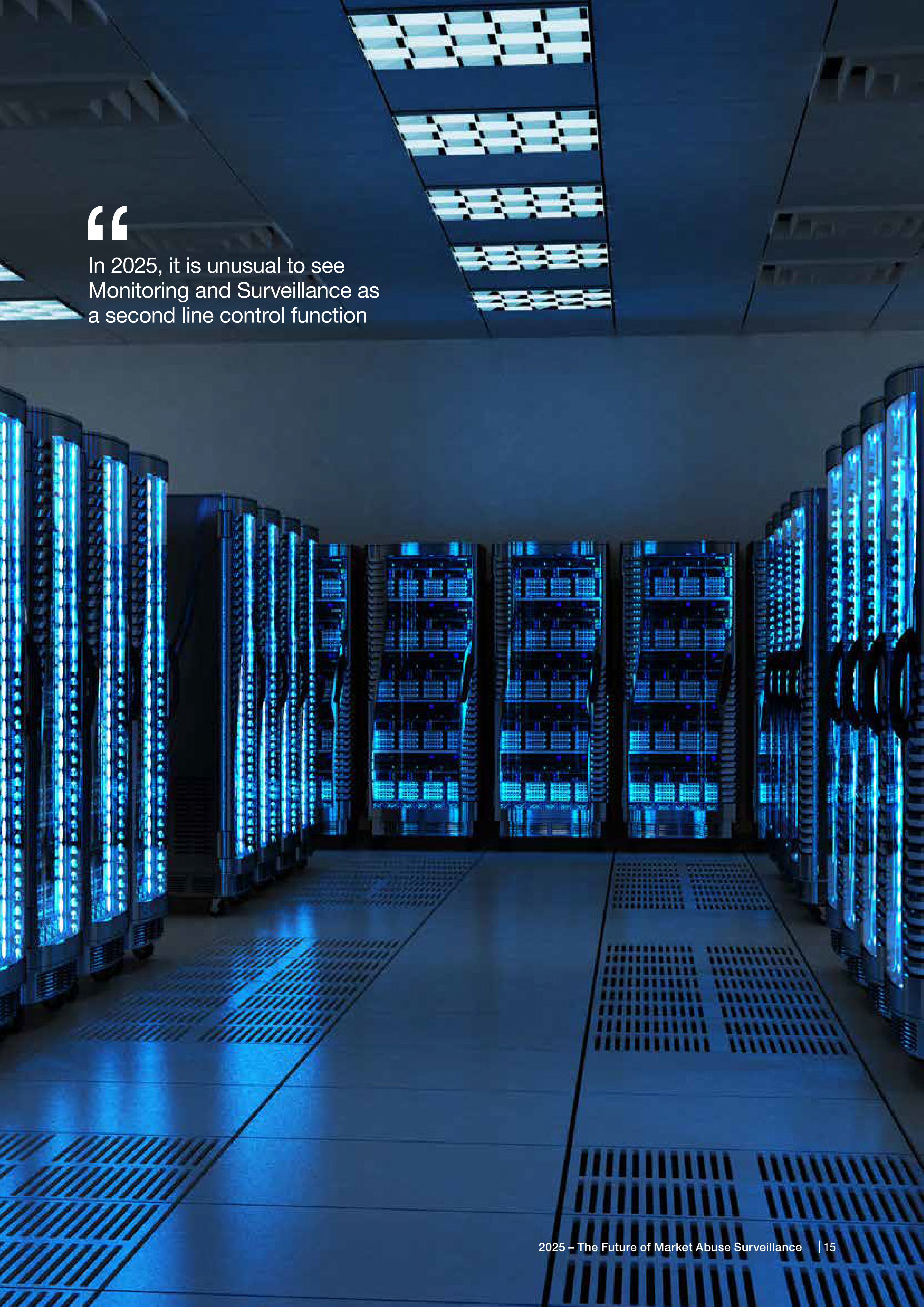
In January 2021, I instigated the first annual 'Monitoring & Surveillance Workshop' and invited not only the programme leads across monitoring, but also key stakeholders from across Compliance, Business Risk Management and Supervisors from the business. The format proved so successful that it transformed into a bi-monthly governance forum after that. The forum discussed emerging risks, control issues, areas of regulator focus and ultimately agreed what 'good surveillance outcomes' looked like for each stakeholder. Roles and responsibilities became much easier to delineate when the group were all on the same page.

My efforts were rewarded and a bank wide strategic transformation project was initiated late in 2021 that saw a consolidation of conduct focused activities into a single monitoring function.

> “
> Ultimately a decision was made to move my function from Compliance into a 1.5LOD reporting line.

Bringing together the different functional activities was not without challenge and ultimately a decision was made to move the surveillance function from Compliance into a 1.5LOD reporting line. My role expanded to be Head of Conduct Surveillance and I had a new reporting line into the Head of Operations. This switch allowed us to better align surveillance and supervision, deduplicate monitoring, and give a clearer view of conduct risk to responsible business heads captured under SMCR in the UK. At the point of transition, my former Surveillance Quality Assurance team remained in Compliance and they continue to perform a more traditional 2LOD role of independently testing and validating our approaches. I don't know whether or not this proved a catalyst event for the industry or whether it was just part of the broader cycle of Compliance periodically moving between the first and second lines of defence, but interestingly the model has been widely adopted and today, in 2025, it is unusual to see Monitoring and Surveillance as a second line control function.

As a second step, I 'cheated' and sought to replicate learnings from my peers. I reached out to my fellow Heads of Surveillance and was delighted by the willingness of the community to meet and share ideas on what good surveillance looked like. I should have bought shares in the various coffee shops, as I moved around the city meeting with the Heads of Surveillance to share my thoughts and to hear from them where they were seeing successes and failures. There are some true champions out there and I found that we typically suffer with similar challenges and were looking at the future in similar ways. In the future, we would come together more often and more formally to provide an industry consensus view of surveillance that had the power to influence both vendors and regulators, but that would take time to evolve.



> “In 2025, it is unusual to see Monitoring and Surveillance as a second line control function

Projects to deliver incremental improvements across the programme

Implementing a cloud based computing strategy

Getting the foundations successfully laid was great, but I was conscious I had committed to a cost neutral surveillance, or as it was now called Conduct and Surveillance Programme. To date my biggest achievement was gaining approval for a costly IT initiative. It was time to get smart and figure out how to remove cost without removing capability and coverage.

Maybe it was a case of right place, right time, but attending an internal conference to hear about a new cross-bank project to consider cloud computing proved to be a game-changer for the strategic path I was to adopt. SaaS offerings were very much in their infancy and although our existing vendors had started to raise the topic in our routine catch-up meetings, we had not thought too much about a full transition or even considered the possibility of such an approach. Looking into our pipeline of enhancements however, it was clear we were being suffocated by the internal costs of technology support, hardware costs and limited support availability which led to unacceptable time lags for implementing enhancements.

We were able to perform our first proof of concept using a full SaaS model in 2022. The speed in which we were able to deploy the test environment was impressive.

A SaaS approach allowed for far more agile changes to be made to the programme and allowed us to explore different approaches more quickly.

The overarching attraction was the potential cost saving which would significantly simplify my budgeting challenges. Hardware costs were all but eliminated and, as importantly in terms of realising cost reductions, we were able to renegotiate licences costs at a significant reduction to previous cost levels. There were ancillary benefits as we also saw a reduction in support headcount. Taken together these cost savings were compelling.

In discussions with our vendors, we demanded two things: solutions had to offer a SaaS model; and secondly, they had to interface with our case management solution. In fact it was not long before the case management solution itself was cloud based. A cloud model allowed us to take advantage of global consistency, of operating our surveillance technology on the very latest versions of the vendors software ensuring we no longer suffered from version control constraints across the regional teams. We could also scale appropriately and pay for what we needed when we needed it.

As we developed the strategy further, our teams took more direct control and through hybrid IaaS and PaaS offerings we were able to run with both the latest models on offer from our vendors and also develop our own models on the same platforms which meant we could apply bespoke alerting to meet emerging risks from within the business.

Consolidated case management and effective MI

Another big and relatively quick win was around our use of case management to provide a single view of alerts. We had started to create a single surveillance case management system before the transition to the new operating model, but the expansion of the function's role accelerated this process. Our expanded coverage required us to review a wider range of conduct risk indicators and it became apparent that the only way to do this was through a trader-centric lens. I couldn't afford to wait three to four years for the data lake programmes to deliver so determined a tactical approach to use case management as a means of getting closer to a single view of trader behaviour by being able to better triage alerts.

As an interim step to bring forward efficiencies, we developed an integrated case management system that allowed us to pull escalated alerts from our trade and e-comms surveillance systems as well as other conduct risk breach information into one place. We leveraged the early progress in the data transformation project to create a single repository to capture all our surveillance alerts. Automated lookups to book static data allowed us to associate trades to individuals or groups of traders running the same book and form a view of an individual's behaviour over time.

When an analyst reviewed a trade surveillance alert in the case management system, the tool automatically flagged e-comms alerts within a similar time window for the same individual. Pulling the alerts together in the case management system auto-closed the alerts in the underlying surveillance tool and we tracked the consolidated case closure through a separate path. Not only did this allow analysts to more quickly access potentially relevant comms when reviewing a trade alert, but it also gave them a better understanding of broader conduct issues by an individual trader over a period of time.

The MI enhancements enabled us for the first time to properly track the effectiveness of our automated solutions and develop feedback loops which would aid in determining the relative strengths and weaknesses of each and every alert. No longer would we fall foul of the non-firing alert for quarter after quarter just to be found out by an Internal Audit review. Furthermore, our analysts felt empowered as the decisions they were making in reviewing alerts was directly influencing the parameter setting of the future.

> “Our analysts felt empowered as the decisions they were making in reviewing alerts was directly influencing the parameter setting of the future.

Delivering cost effective outcomes based Comms surveillance

E-comms surveillance was the most resource intensive element of the current set up, with more than 50% of the global surveillance team reviewing alerts which were surfacing a range of creative profanities but next to nothing in terms of actual cases of market abuse. Worse still, with my purview having extended to Conduct and therefore to monitoring of employees across the bank, e-comms surveillance was going to take up an even more of my budget which felt disproportionate.

The analysis performed during the external review in 2020 had been helpful to benchmark our programme, but it did not go far enough to radically change the alert levels. I needed to act. I considered a brutal review and cull of the size of the lexicon but quickly realised this was only going to provide marginal gains at best.

I did my homework and saw many vendor solutions and spoke to my peers on the choices they had made. I was intent on reducing my reliance on lexicons and favoured adoption of natural language processing (NLP) techniques. But I wanted more than better e-comms software; I wanted a solution that delivered less alerts, more true positives, the flexibility to build and deploy new models targeted at new or heightened areas of risk, and I wanted it all at a lower annual cost.

The improved confidence that my stakeholders had started to show in the surveillance programme gave me the opportunity to push what even I regarded as a radical idea. Firstly we changed the focus of comms surveillance from a purely detective control to add an ‘early warning system’ by identifying upcoming risks at the earliest stage through the communication channels.

> “
> The savvy banks have been able to balance the cost saving opportunity with the extension of process coverage by applying relevant and appropriate bots.

Secondly, I resolved to deploy a managed service solution and was persuasive in my arguments. We opted for a managed service solution for first level alert review and implemented an enhanced technology solution with support from our managed service provider who then took primary responsibility for, at our direction, maintaining and optimising the solution. After the initial set up, this delivered a significant simplification of our operating model and allowed us to reduce overall headcount and focus on higher impact activities.

Voice surveillance technology had lagged behind its e-comms cousin and pre-2021, we were relying solely on manual reviews, with our analysts listening to replays of calls. The effectiveness of our surveillance in respect of a-comms came into question in the 2020 FCA STOR visit.

Harnessing RPA

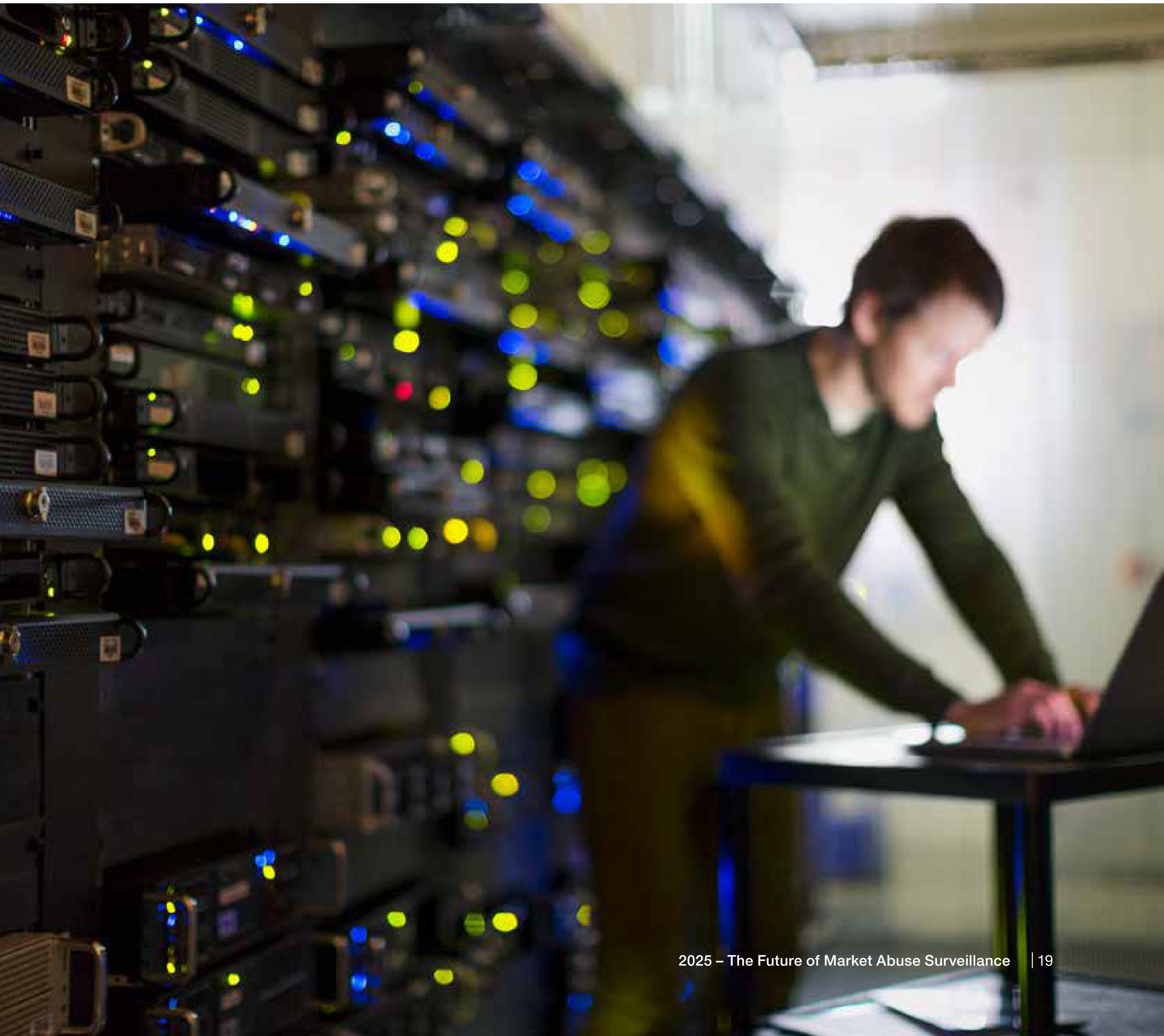
Although we needed to start to extend the level of coverage and in doing so moving to a fully automated solution, we were able to make some initial progress almost immediately through leveraging our growing RPA programme. Robotics had been heralded as the next big thing back in 2018-2019 but results in Surveillance had been decidedly mixed.

The savvy banks have been able to balance the cost saving opportunity with the extension of process coverage by applying relevant and appropriate bots. I set out to support manual controls where it typically took more time to collect the data than actually performing the review itself. And tactical manual controls over voice surveillance was a good place to start.

We replaced the manual selection and collection of voice tapes ahead of review by adopting a bot called ‘Cicero’. By firstly applying metadata attributes to select potential calls for review based upon a higher risk population, and the time of call, length of call and participants, the metabots selected the sample and then automatically collected the call file. This proved a good sticking plaster.

Ultimately in late 2023 we chose to outsource voice surveillance as well, the decision was made easy as our e-comms vendor solution had developed impressive a-comms transcription capabilities which existed as an extension of the core software, albeit with an additional license cost. Given the increase in working from home post Covid we had seen an exponential increase in video calls and the software dealt with this. Video calls had led to an increase in overall voice traffic and arguably greater risk so the ability to move away from sampling and review everything at a palatable price point through the managed solution was a considerable benefit.

The partnership with my managed service provider has been successful. I have reduced the bank's headcount, and in my opinion have reduced risk courtesy of the SLAs in place which give me comfort over the quality and reliability of the service I receive while also leveraging market leading technology. Critically it has also allowed us to focus on the analytics which in the discipline of surveillance is of course what it is ultimately all about.



Deploying behavioural analytics

Development of the Surveillance Control Tower and behavioural analytics

My central premise was that market abuse is perpetrated by individuals, and that therefore in order to detect market abuse, it was necessary to be able to apply a trader-centric lens. And that meant being able to monitor behaviour and how that behaviour manifested itself as trading activity. Understanding behaviour meant being able to identify subtle and connected events and the patterns they formed over time.

While trade surveillance vendor technology was increasingly evolving and adopting machine learning alongside more traditional deterministic rules based approaches, I wasn't sure that any single vendor could meet my aspirations for a behavioural system and ingest and combine all the data sources that I had in mind. Equally I wanted to step away from the model in which I had to review every alert generated in the full knowledge that almost everything would prove benign. It was time to challenge the prevailing orthodoxy that it was imperative to review every alert.

This thinking was the genesis of our Surveillance Control Tower. We developed our own internal bespoke analytics layer. This became the nerve centre and intelligent eyes of the Surveillance function monitoring traders and trading activity, underpinned by the data made accessible through the data lake.

The Control Tower consolidates trader activity, surveillance alert outcomes, comms meta-data, P&L, positions data and a host of data artefacts, for example conduct breaches, which we think have value in building a profile. This allows us to create a trader-centric view covering a wider range of behaviours. Rather than looking for a single point in time event highlighted through the triggering of a rule based upon a single market abuse behaviour, we have the ability to combine various signals across structured and unstructured forms of data to classify patterns of individual events, namely behaviours, as either normal or potentially anomalous.

We perform a range of analytical techniques layering analytics to isolate behaviours of interest, for example a trader trading more aggressively or in different instruments, and in doing so deviating from their normal mode of activity.

Vendor surveillance solutions still exist and play an important part within the surveillance ecosystem, but they now fulfil a different role. Rather than being the sole determinant as to whether a sequence of orders or trades are outliers against the parameters set within the model, they are one of a number of signals provided to the Control Tower. In our brave new world vendor solutions provide signals, but decisioning has been passed to the Control Tower which is where signals are combined and insights generated.

As a result we don't review all the alerts generated by our trade surveillance vendor solutions any more. The Control Tower builds patterns and visualises behaviours which are ultimately risk scored. Higher risk scoring alerts that exhibit the characteristics of a potential market abuse event are prioritised and sent to our specialised review teams. This led to more time being spent investigating a higher risk alert population.

It took time to get global regulators comfortable with this approach and for a period of time we parallel ran our risk based approach with a review of traditional alerts. What we were able to demonstrate is that we prioritised everything of consequence alerted out of our vendor based solution as individual signals derived from the vendor platforms were amplified by a wider set of signals identified through our contextual and behavioural profiling. Perhaps most importantly the proof was there for all to see. Our Surveillance Control Tower identified more genuinely anomalous behaviour and for a period of time our volume of reported STORs dramatically rose. Put simply our approach was working.

Surveillance Control Tower and behaviour analytics

If the conduct and compliance-centric data lake is the heart of a market abuse surveillance solution, then the Surveillance Control Tower is the brain. The large amount of interrelated data in the lake needs an analytics layer to intelligently identify patterns of behaviours and more importantly, changes in those patterns that can indicate abuse. It will be possible to predict emerging behaviour patterns using inputs such as employee performance to allow proactive early identification of concerning behaviour as opposed to traditional retrospective identification of potential abusive behaviour.

In order for the Control Tower to be effective, a rather unusual approach is needed. The traditional approach to surveillance involved tuning surveillance models to produce only the most abusive events for review. The Control Tower requires a broad set of input signals which can be used to build up profiles of behaviour patterns. This can be achieved through detuning surveillance models; what was once considered a false positive alert is now a crucial data point to understand an individual's trading patterns and therefore what is unusual and worth investigating. The bi-directional nature of the data lake allows behaviour patterns to be fed back in and incorporated into increasingly sophisticated analytical models.

Using the underlying data in the data lake and the analytics performed by the Surveillance Control Tower can solve complex problems such as collusion detection as shown in the example below, and the same techniques would be applied to solve other challenges such as detection of cross product and market manipulation.

The three crucial building blocks to any Surveillance Control Tower must be, greater contextual information, analysis of behaviour patterns and risk rating the severity of the perceived abuse to direct investigation.

Greater contextual information

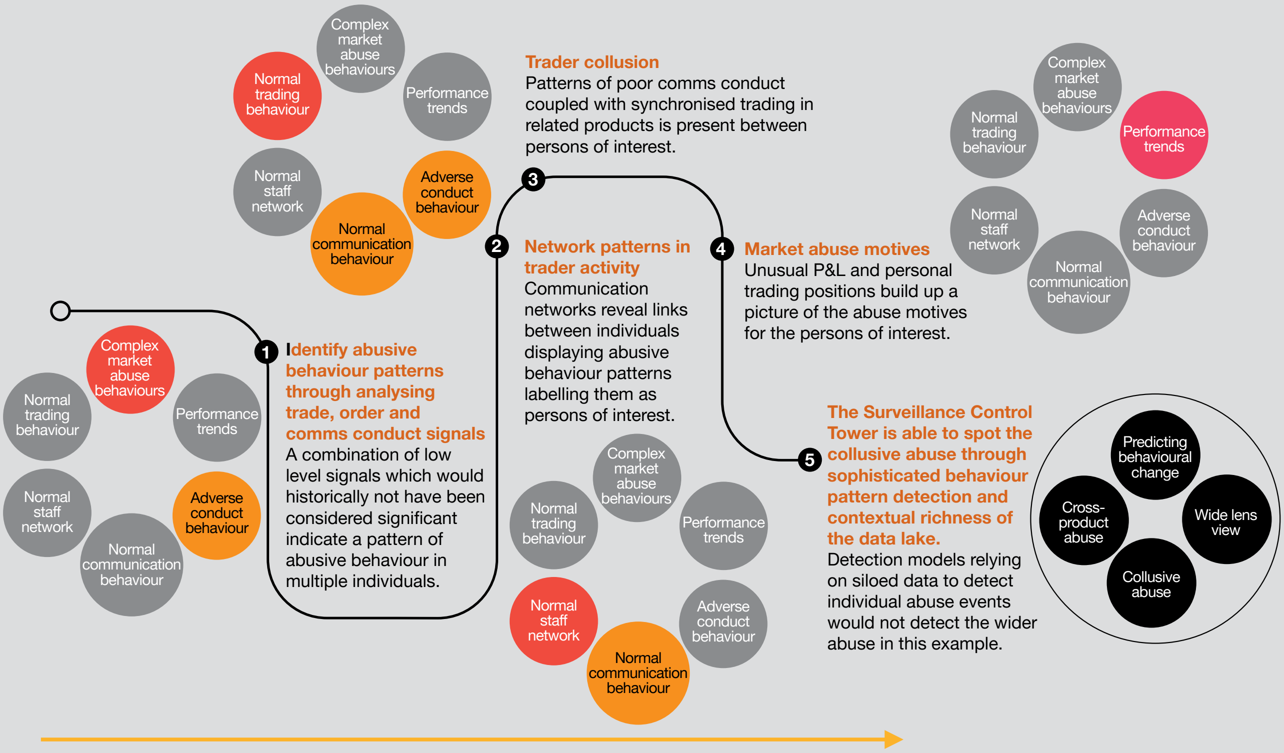
The addition of contextual data to market abuse surveillance provides a greater range of abuse indicators for use by control tower analystsand automated models.

Behaviour pattern analytics

Taking a more rounded view of an individual's past and present activity to decode more subtle indicators of abuse. Individual events, traditionally regardedas false positives, act as valuable indicatorsof behaviour patterns which when combined improve abuse detection.

Risk based analytics and scoring

Stepping away from the notion that 'all alerts are equal' in order to drive a more risk weighted view of detection, essentially prioritising higher risk incidents.


Complex market abuse behaviours
Normal trading behaviour
Performance trends
Normal staff network
Adverse conduct behaviour
Normal communication behaviour
1
2
3
4
5
Predicting behavioural change
Cross-product abuse
Wide lens view
Collusive abuse

1 Identify abusive behaviour patterns through analysing trade, order and comms conduct signals
A combination of low level signals which would historically not have been considered significant indicate a pattern of abusive behaviour in multiple individuals.

2 Network patterns in trader activity
Communication networks reveal links between individuals displaying abusive behaviour patterns labelling them as persons of interest.

3 Trader collusion
Patterns of poor comms conduct coupled with synchronised trading in related products is present between persons of interest.

4 Market abuse motives
Unusual P&L and personal trading positions build up a picture of the abuse motives for the persons of interest.

5 The Surveillance Control Tower is able to spot the collusive abuse through sophisticated behaviour pattern detection and contextual richness of the data lake.
Detection models relying on siloed data to detect individual abuse events would not detect the wider abuse in this example.

Understanding risk and dynamically responding to it

Another of our challenges was dealing with the volatility of the markets and heightened risk profiles arising from rapid movements in market sentiment. Covid highlighted the limitations of traditional surveillance. During March and April 2020 our static alert calibrations were rendered ineffective for certain behaviour types where trading levels exploded. Our only solution at the time had been to de-prioritise some coverage to avoid unmanageable volumes of alerts being generated.

We had no mechanism for more dynamically adjusting the hundreds of models we were running and in any event our governance processes constrained our agility to make rapid changes. Again the Control Tower has proved to be the solution. Taking a behavioural approach we were able to begin by applying filtering techniques, using relevant indices and benchmarks to calibrate for market movement and remove a layer of alerts which we considered to be lower risk. As we got more sophisticated we started to apply different sensitivities to tune out alerts generated by extreme market movements and to apply machine learning algorithms to react to market events and make determinations as to where calibrations should be set. Within the Control Tower, the MI we have built allows investigators to playback settings and over-ride the algo calibrations to apply judgmental calibrations and a more conservative lens through which anomalies can be identified and reviewed. In line with IOSCO standards our Compliance's QA team uses the same features to independently test the design and operational effectiveness of the algorithms.

The Control Tower is continually involving and has and will continue to revolutionise our surveillance capability. They say that imitation is the sincerest form of flattery; a number of our peers are now building their own Control Towers.

Delivering on Conduct surveillance

The respect and confidence now being shown in the Surveillance function from across all our partners and stakeholders has certainly elevated the impact we now have with a broad number of open interactions and new projects in place. This was initially seen when the first line supervision teams approached us to jointly develop enhancements to their Conduct Risk dashboard by adding surveillance findings to the coverage. The engagement was successful because we not only managed to create a feed to give a view, but we designed the process for a feedback loop from the supervisory reviews back into the Surveillance Control Tower which completed the circuit and enabled new integrated alerts for both the 1st and 2nd lines of defence to consider.

More recently, the creation of a Conduct and Culture programme within the bank, owned and chaired by the Head of HR and Employee Engagement has enabled us to play a very different role to the traditional surveillance team that looks only for poor behaviour and/or conduct.

In taking good conduct and culture as indicators of a strong and trusted organisation we look to seek competitive advantage from being able to display examples both within and outside of the firm. The Control Tower has provided a lens for the bank to be able to identify instances of good conduct and culture through the behaviour of our employees, as a delta to the core programme. These messages are used by the Head of HR and Employee Engagement and his committee to demonstrate the significant number of employees showing core values. Surveillance has also become value additive to the business and behavioural profiles are starting to be used to understand performance and client engagement. Surveillance is increasingly being used to help the first line understand clients' needs and patterns of behaviour better and to help traders make better decisions translating those to alpha. With each new success comes greater attention, greater support and greater funding.

Reflections from the summit

Reflecting on my five years in role the time has flown and I've no doubt that our surveillance capability has transformed. The journey has been hard, with ups and downs, but I wear the stress earned grey hairs as a badge of pride. I am comfortable in the assertion that as a consequence of the transformation programme we have undertaken, we have a conduct and surveillance ecosystem capable of detecting all forms of market abuse.

Not that I am complacent. There is no room for complacency in this role and despite horizon scanning there is always the risk of the unexpected. We struggled with providing surveillance over crypto currencies and in particular with crypto derivatives and the risk of creating and abusing dominant positions. We are still working with the industry today to create the common reporting standards necessary to fully mitigate the evolving suite of crypto specific market abuse scenarios.

Our CCO has just moved on to a new role, but in her leaving speech she stated how "*better surveillance, lower cost*" had been her persistent mantra to me and that I had exceeded her wildest expectations and set a very high bar for the Head of Surveillance at her new shop. She was kind enough to point out that in the last five years the implementation of our incremental transformation programme had led to a 60% reduction in false positive alerts and that we had more than doubled the number of STORs we reported in the previous year. All the while remaining cost neutral comparing 2025 with 2020.

With that praise still ringing in my ears I was the recent recipient of a STOR visit. It was a very different conversation from five years ago. My team were keen to showcase the capabilities we have developed, and the depth of their expertise. Strangely a lot of the conversation focussed on the culture of the organisation, our escalation process and the thresholds we set for raising a STOR. I realised that the angle of questioning was being driven by the marked increase in the number of STORs we had raised in the previous year. I articulated that the increased number of STORs had been a function of the sophistication of our analytics. Along with my peers at other banks I had always speculated as to how much market abuse went undetected, especially in difficult to detect areas such as abuses across correlated products and the Control Tower had given me the answer. I concluded my answer to the FCA by stating that STORs relating to our own traders' activities had dropped in 2025, which I ascribed as being down to the culture of the organisation and a recognition that our detective capabilities had never been so good. The answer was obviously satisfactory as when we received feedback from the STOR visit it was glowing. It was the ultimate vindication of my efforts.

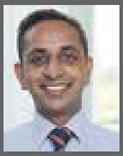
Later, as I mused on the STOR visit, it struck me that perhaps the FCA had been asking the wrong question. Perhaps it wasn't a case as to why I had been raising so many STORs but rather why had some other organisations been raising so few....

> Along with my peers at other banks I had always speculated as to how much market abuse went undetected, especially in difficult to detect areas such as abuses across correlated products and the Control Tower had given me the answer.

Contacts

Graham Ure
Partner
graham.ure@pwc.com
+44 (0) 7889 644672

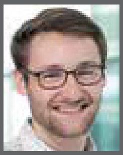
Stephen Livermore
Special Advisor
stephen.livermore@pwc.com
+44 (0) 07585 120800



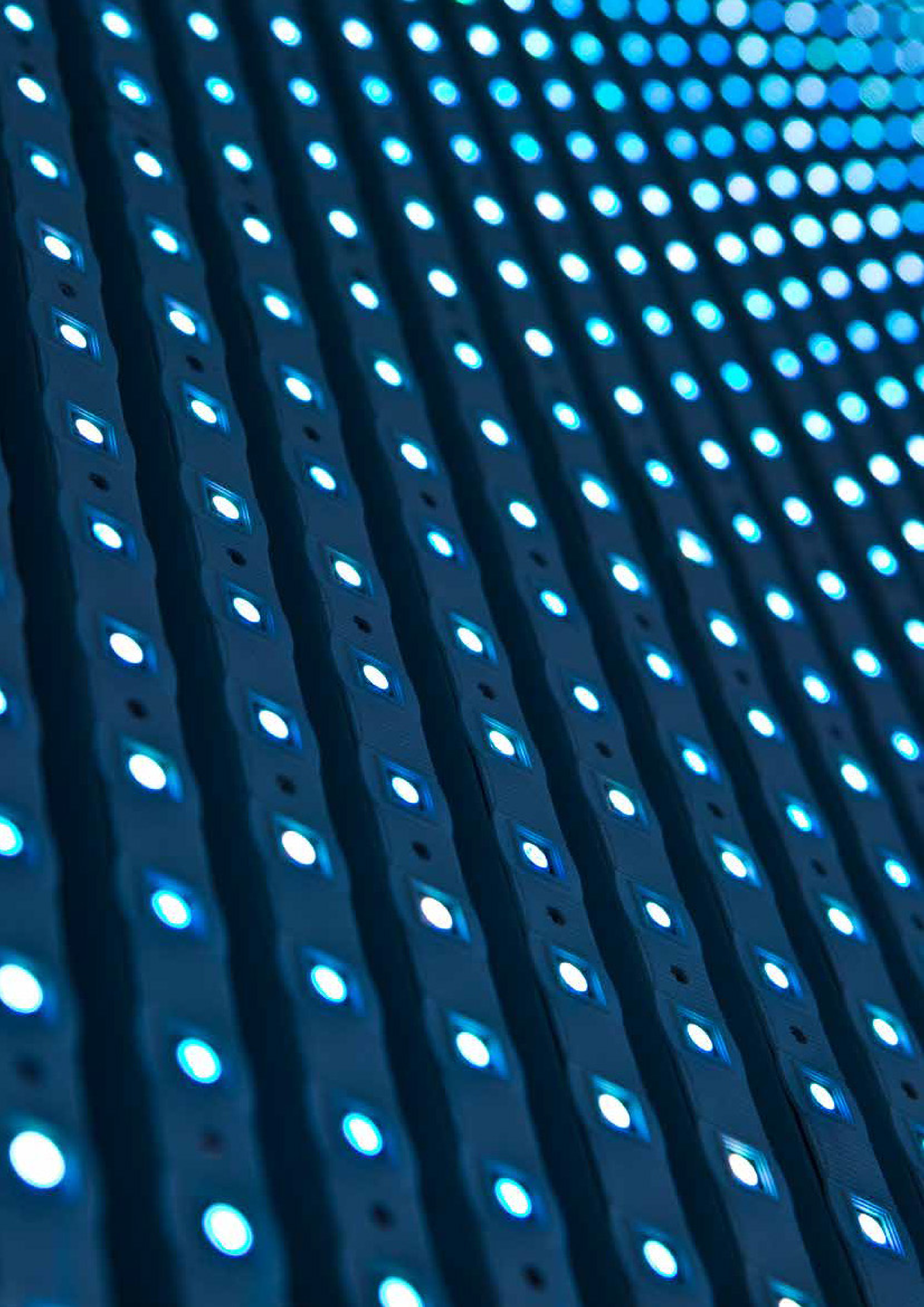
Ruk Permal
Partner
rukshan.permal@pwc.com
+44 (0) 7595 611533

Alex West
Director
alex.e.west@pwc.com
+44 (0) 7841 567371

Mark Chopping
Director
mark.chopping@pwc.com
+44 (0) 7889 645115



Rob Lloyd
Manager
robert.a.lloyd@pwc.com
+44 (0) 7802 660239



www.pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

Mitie Design RITM4059546 (11/20).