afme/
Finance for Europe

KPMG

The Future of Surveillance in Wholesale Banking

October 2019

afme/ Association for Financial Markets in Europe
www.afme.eu

Contents

Disclaimer

October 2019

1 Foreword

AFME is pleased to publish "The Future of Surveillance in Wholesale Banking" in collaboration with KPMG. This report comes at a pertinent time in the evolution of the surveillance function.

Following the financial crisis and subsequent conduct issues, the industry has significantly increased its focus on surveillance to detect market abuse, market misconduct and financial crime. Across Europe, the implementation of the Market Abuse Regulation (MAR), as well as the Fourth and the Fifth Anti-Money Laundering Directives are a key part of this.

Emerging technologies, such as machine learning and network analysis, may offer firms the ability to more effectively monitor the constantly evolving patterns in communications and trading, as well as reduce reliance on manual processes and increase efficiency.

However, further developments are necessary for surveillance to be consistently effective. Improved data and new skillsets of staff are key, as is investment funding at a time of many competing needs.

This paper outlines some of the key points to consider, when planning a future surveillance strategy, as well as emphasising the challenges that firms may face.

The nature of surveillance means that its evolution is uncertain and therefore open to debate. Nevertheless, we hope that this report will be a valued contribution to ongoing discussion.

AFME would like to thank KPMG for their efforts in compiling this report, as well as members from AFME's Compliance Committee, Compliance Issues Working Group, Surveillance Working Group and, all of whom made contributions that were integral to the development of this publication.

James Kemp
Managing Director
GFMA and AFME

2 Executive summary

Surveillance within wholesale banks is integral to the identification and investigation of unlawful or unethical practices, such as: misconduct, market manipulation and market abuse, and financial crime. The surveillance function in financial institutions has evolved significantly over the last ten years, mainly driven by regulatory requirements and high-profile misconduct cases. Banks have, as a result, invested heavily in building their surveillance capability. However, with rapidly developing technologies and regulatory expectations, the ongoing drive to enhance the effectiveness and efficiency of surveillance must continue.

In this paper, we discuss how the surveillance function may develop in the coming five to ten years. The information in this paper is based on the opinions of well-informed and experienced industry professionals from over twenty banks, obtained through a series of interviews with AFME members of various size and scale, with a geographical spread of head office locations, including France, Germany, Italy, the Netherlands, Switzerland, Australia, the UK, the USA, Canada and Japan. A complete list of AFME members can be found at www.afme.eu.

The following themes were addressed: the role of data, the impact of technology, the skills of surveillance officers, the future state operating model and how the industry can work better together.

The figures in this paper are based on the results of questions answered by interview participants.

Our key insights are as follows:

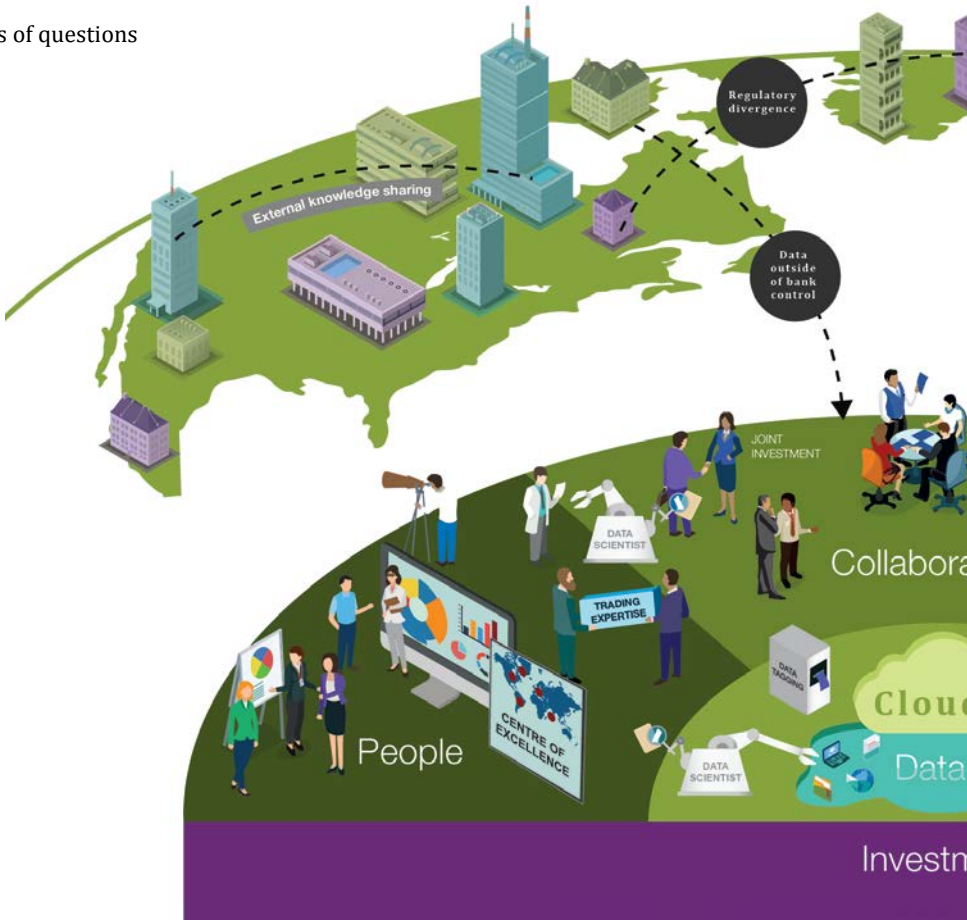
01 | Improved data integration is now vital to enhance value

The quality of an organisation's data will become its biggest differentiator. The market-leading banks of the future will be those most able to trust their data, link data points together and enrich with wider behavioural and organisational data from Human Resources (HR), Risk and other business functions. Access to an increased number of data points (for example: communications, trade, orders and quotes) has the potential to widen the scope of surveillance – linking potential market abuse risks to conduct, financial crime and non-financial risks.

02 | Surveillance will require access to a common data layer

Banks desire a flexible data utility, whereby data can be sourced once and used many times across different functions. Surveillance will be one of many beneficiaries within the bank which will draw value and insight from the data asset.

What could the future of surveillance look like?

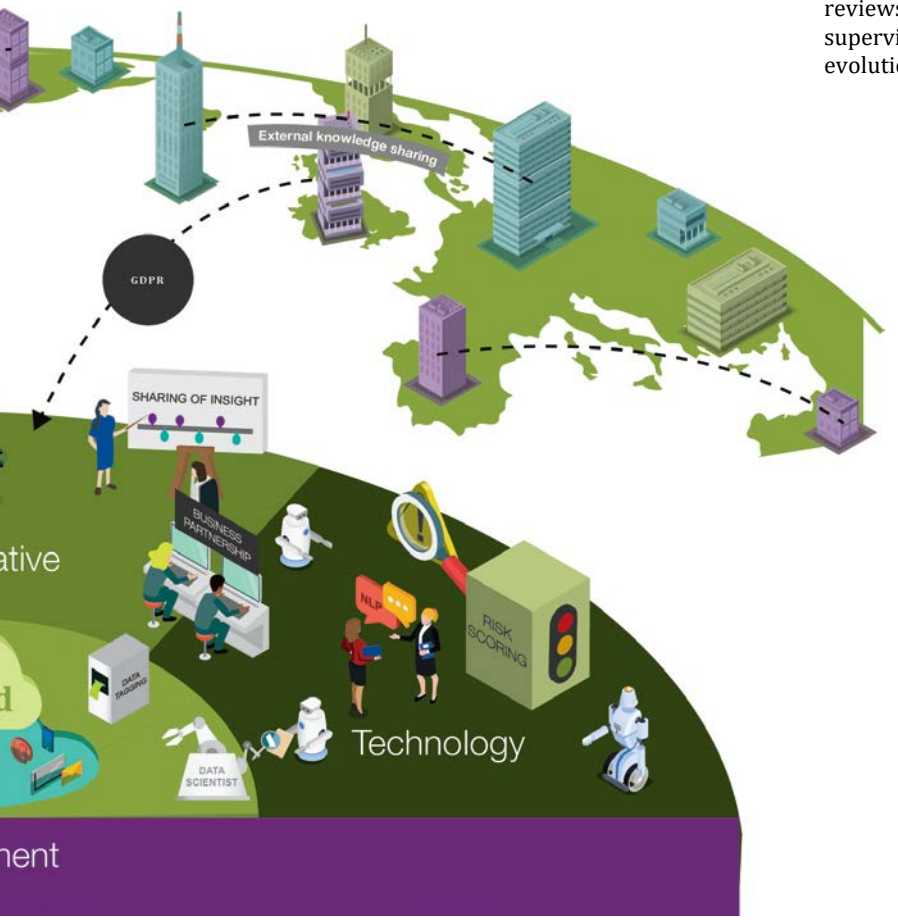


03 Technology will accelerate the move to more efficient risk-based surveillance

The application of new tools and technologies, such as machine learning techniques, improved analytical models and network analysis, will enable computers to understand the context of the data they are processing. Technologies that support artificial intelligence and machine learning will increase scalability and lower the cost of performing surveillance. These advances in technology will allow for more sophisticated techniques to analyse and signal behaviours and trading patterns. The result will be greater efficiency, earlier risk detection and, in some cases, prevention.

04 'Centres of excellence' will replace traditional high-volume operations centres

The current process generates a significantly higher proportion of false positives and is limited in its ability to be further optimised. The drive towards more intelligent alerting mechanisms and automation of some of the operational tasks which are performed by analysts today necessitates the implementation of a more investigative review process in banks, applying expert judgement to join various data points together. This could reduce or completely replace the high-volume alert model.



Future surveillance professionals will be required to excel in technology-centric areas, such as: data comprehension, data processing and data law. These skills will be highly prized

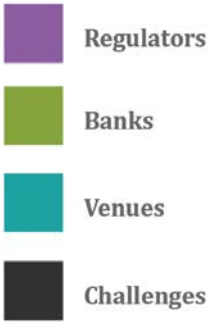
05 Surveillance will be recognised as a business partner

Increased access to front office technology, and vice-versa, will allow for better integration of solutions and lower implementation costs for surveillance functions and organisations overall. More sophisticated techniques to detect unfamiliar behaviours and/or trading patterns will allow surveillance functions to escalate findings to front office supervision sooner.

06 The benefit of greater industry collaboration and new alliances

Greater consistency in surveillance practices across the industry should be driven by a more open and systematic way to share best practice and lessons learned, developing more robust and effective surveillance processes.

Trading venues and regulators, as custodians of consolidated data sources, have a role to play in driving the surveillance of wider risks, which banks are not able to detect individually. As the future of surveillance shifts away from alert-based reviews towards intelligence-led techniques, regulators and supervisors will need to become comfortable with this evolution and permit the switching off of existing systems.



3 Background and current state

The surveillance function in financial institutions has evolved significantly over the last ten years. Driven by regulatory compliance requirements, it facilitates and underpins the investigation of practices which include misconduct and market abuse.

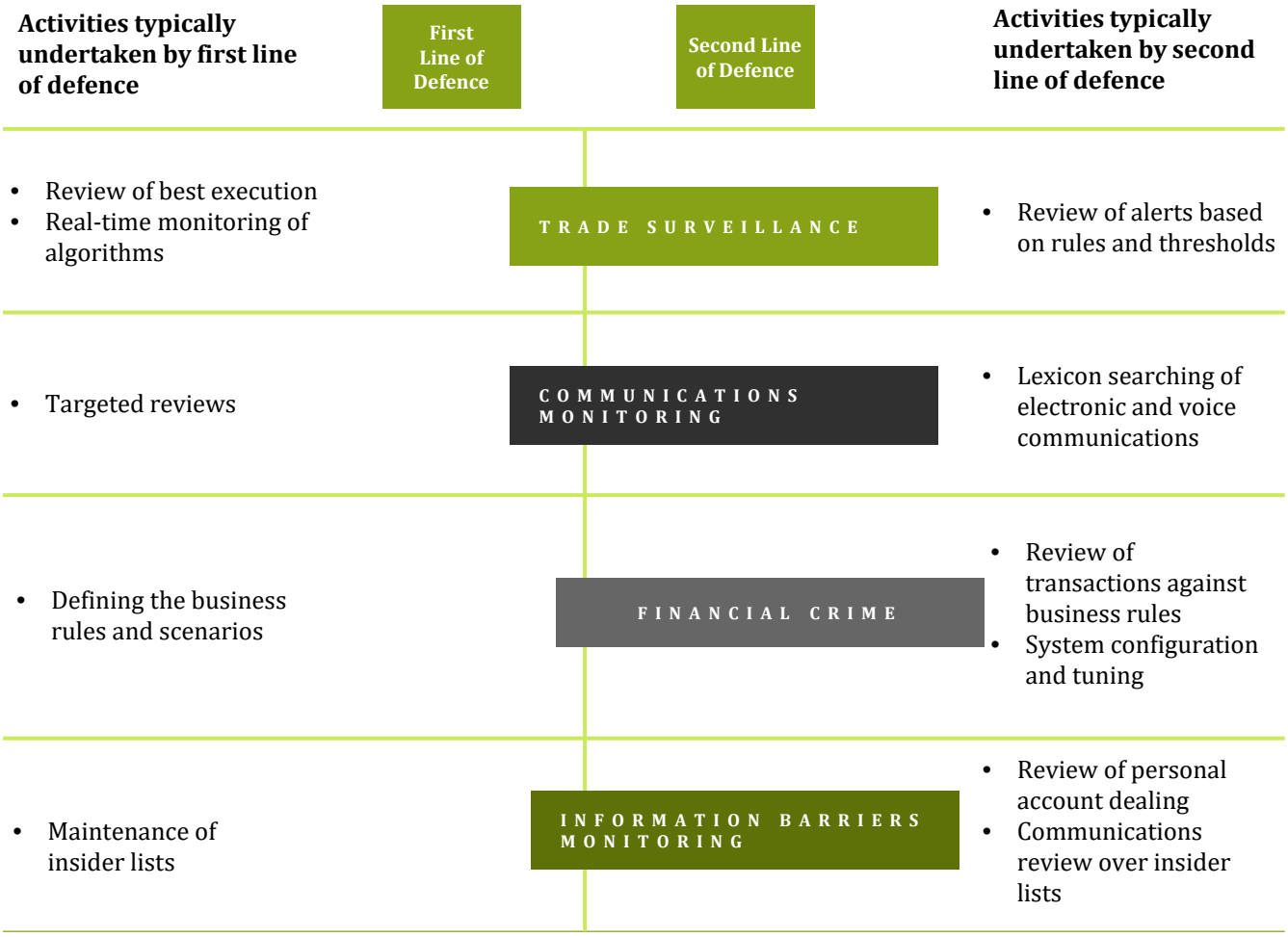
Effective surveillance plays a key role in safeguarding a bank's internal reputation and in building public trust in the industry. Clients are more likely to have confidence in transactions with a bank if they know that comprehensive surveillance techniques are being applied. Also, the better the data a bank possesses overall, the better the service it can provide to its clients.

Regulatory focus on market conduct has intensified since the financial crisis. Between 2011 and 2016, including regulatory fines and remediation costs, the global cost of market misconduct for banks is an estimated $375billion[1].

The implementation of the Market Abuse Regulation (MAR), the Fourth and the Fifth Anti-Money Laundering Directives in Europe have necessitated further surveillance solutions in banks to ensure compliance with a broad range of requirements. However, globally, there is no unified approach or standard for surveillance. For banks that operate across multiple jurisdictions, surveillance needs to take account of evolving expectations from international regulators, industry participants and the general public.

In addition to completing the latest round of regulatory compliance programmes, banks are increasingly looking to improve and automate risk detection capability and realise their investment in surveillance solutions, as well as to close residual compliance gaps.

The following diagram shows where a surveillance function usually sits within a bank's standard 'three lines of defence' model and which activities typically form part of a bank's surveillance approach:



Note: 1. Source FICC Market Standards Board Annual Report 2017.

The table below highlights key drivers of change and challenges that are impacting the current operating model of surveillance functions:

Driver	What are the challenges?
Strategic vision	Evolving regulatory requirements and market wide remediation activities, sometimes required at short notice, have often forced surveillance functions to juggle between implementing their strategic vision for the future and making tactical enhancements to existing processes.
Increasing expectations to detect risks	Expectations of surveillance functions, from bank management, regulators, clients and the general public, are high and increasing. As new risks emerge, the surveillance function will be expected to expand further, encompassing new prohibited behaviours[2] as well as wider conduct issues that threaten the reputation of the bank, such as non-financial misconduct.
Process efficiency	Across the surveillance function, current processes generate high volumes of alerts, most of which are false positive. Additionally, due to differences in the data sources and monitoring systems, communication and trade surveillance are often performed by separate teams with limited overlap, sometimes in off-shore/near-shore centres. For the small number of genuine issues identified, this consumes significant resource and is an expensive process to run.
Availability of data and technology	Banks are using third-party vendor solutions comprising rule-based alerting systems, focusing on specific market abuse scenarios. There are some sophisticated technology solutions emerging from vendors, including statistical model-based methods to detect anomalies alongside traditional rule-based alerting. However, in order to fully realise this potential a high quality, rich and complete data set is required, which in practice is not always available – for example, due to the lack of data granularity for OTC products. Communications surveillance often utilises a lexicon of search terms which are applied across communication channels to identify high risk communications for review. This approach relies on simple search and text pattern matching and results in a high number of false positives. With the emergence of new technology allowing firms to analyse additional data from communications, such as sentiment, banks are considering how they can use this technology to drive better risk detection and process enhancements.
Bank wide cost pressures	Consuming a significant volume of resource and implementing big-ticket technology - surveillance is expensive. As banks seek to improve their returns on equity, surveillance functions will continue to face cost pressure and scrutiny of the funding they request to execute future state strategy.
Coverage and consistency	The monitoring of financial crime and market abuse risks are run as separate processes at almost all banks interviewed, reflecting the differences in data requirements and underlying rules. There are some examples where forums exist to share knowledge - for example, market abuse STOR information that may be used to assess whether further investigations are required from a financial crime perspective. However, there is currently very little synergy.

Note: 2. Flying Prices and Printing Trades' from FCA Market Watch 57
Source: https://www.fca.org.uk/publication/newsletters/market-watch-57.pdf

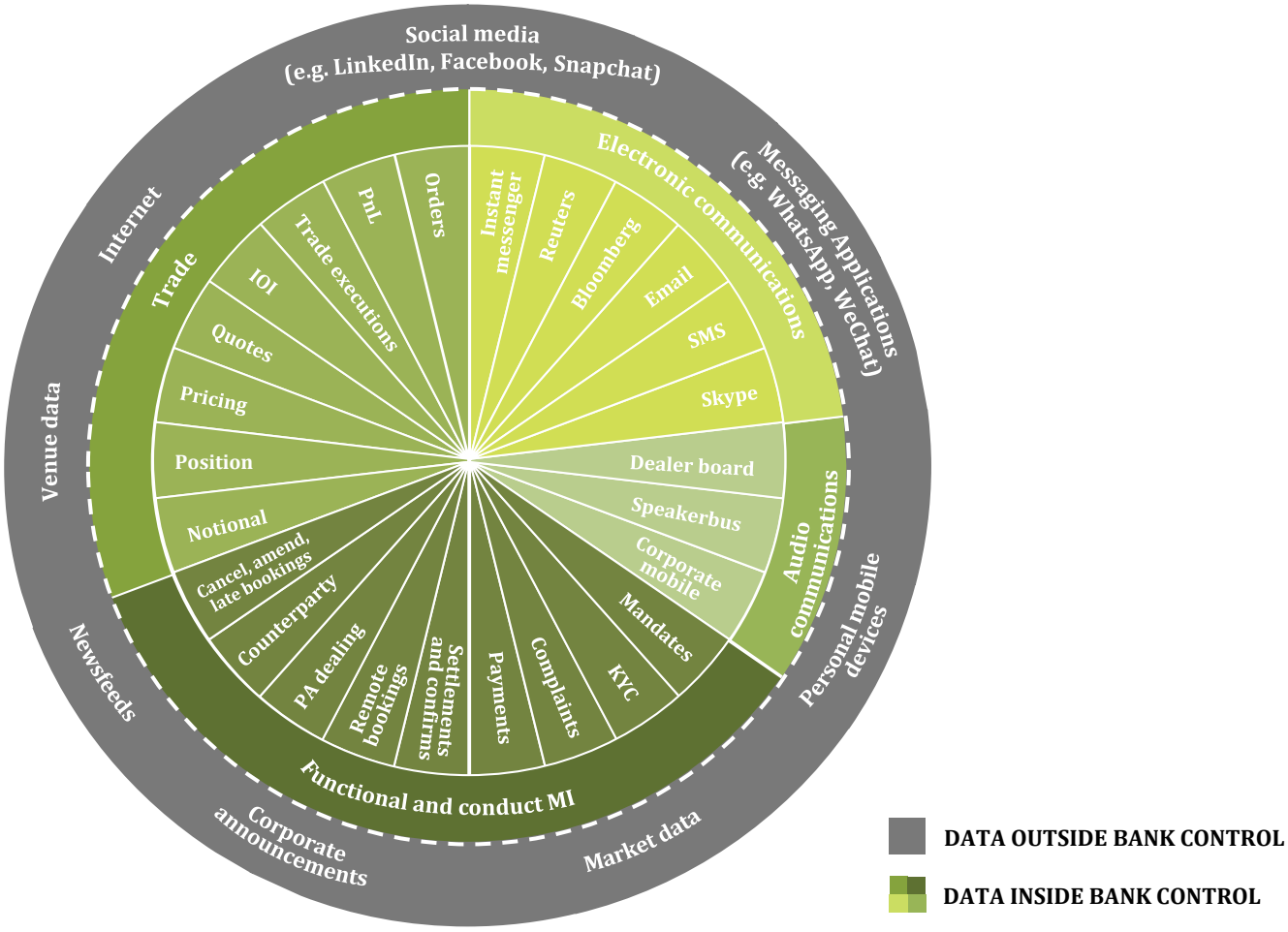
4 Critical role of reliable and comprehensive data

4.1 Data as an asset

Banks recognise the value of their data, even if they face challenges in accessing it. Complete, accurate and trustworthy data will deliver results that can benefit the whole business, not just surveillance. There is a direct correlation between the effectiveness of a bank's outputs and the quality of the underlying data inputs

Currently data exists in a raft of bespoke and legacy systems, because of mergers and acquisitions, as well as responding to short term regulatory pressure. Banks have established extensive programmes to clean up their legacy architecture, enabling them to process data in significant volumes. Sourcing better quality data will benefit individual functions and the whole organisation. The collective analysis of which will enable efforts to be focused on higher risk data points.

The following diagram provides an illustration of the types of data that could be consumed by a surveillance function:



The below table highlights some of the key data dependencies for second line surveillance and monitoring functions when relying on data from processes within the first line:

Key compliance surveillance and monitoring controls	First line data and process dependency
Trade surveillance	— Timely, accurate and complete trade, order and quote capture. — Timely and accurate counterparty set up. — Review and application of pricing and mark ups.
Communications surveillance	— Review of communications.
Financial crime	— Counterparty set up and client on-boarding. — Trade settlement and payments.
Control room	— Disclosure of personal accounts and periodic attestation.

4.2 Data strategy

The way surveillance functions access and use data will transform as data strategies in banks evolve. Once banks can consume data more readily, they can build more integrated surveillance controls that consider a range of indicators. This will reduce false positives, focussing on true anomalies.

Over 80% of the banks interviewed envision that their surveillance data will be sourced from an integrated, cross-functional data utility as an alternative to creating a surveillance-function specific data repository.

The table explores these data strategies further:

Surveillance primary data source	Ownership of Data Strategy	Advantages	Disadvantages
1. Cross-functional data utility Single data layer which can be accessed by different functions across the bank.	Technology	— Source once, use many times across wider organisation, making the data more reliable. — Senior Manager support will ensure buy-in from other functions (e.g. HR business and IT). — Cost effective for surveillance functional budgets.	— Significant effort required to normalise a wider data set. — Longer time frames to implement due to the amount of data being incorporated. — Less tailored to surveillance specifications.
2. Surveillance function specific Data sourced specifically for surveillance.	Compliance/ surveillance	— Tailored to surveillance specification. — Can be executed in shorter timeframes (provided there is support from the business/IT).	— Lack of support from business and IT may create unnecessary roadblocks such as time delays, IT resource reallocation and budget push back. — Costly for an organisation to maintain multiple data silos.

Joined-up data can give valuable insight

Banks can gain more value from high quality data which allows the joining of different data sets together to create more insightful information that will drive both commercial and control decisions.

Banks expect that a fully holistic surveillance solution is not on the five to ten-year horizon, however improvements in the availability and quality of data are likely to push surveillance capability forward in this direction. At a minimum, banks expect to have access to a wider data set in the investigation of alerts.

The diagram below outlines the various phases of maturity that a surveillance function is likely to move through over the next five to ten years:

Organisational alignment of surveillance teams

— Access data across the functional silos (between communications and trade monitoring).

— Investigative approach to alerts which ensures data can be accessed and analysed.

Ability of surveillance function to access other organisational data

— Access to wider organisational data to aid in the process of closing alerts (e.g. KYC, sanction screening, training records, risk limit breaches, etc.)

Utilisation of common data layer

— Common data layer bringing all control function and business data together in a single view.

Automation of data linkage

— Rules/logic or artificial intelligence to automatically link data points.

4.3 Transition to the cloud

Data strategies are being influenced by cloud.

Banks are considering, or are in the process of, transitioning to the cloud. They cite greater scalability and cost effectiveness as key potential benefits.

Cloud-based solutions can provide many benefits, such as:

- ✓ Increased scalability
- ✓ Faster processing power of larger data sets
- ✓ Access to market leading technology applications and cognitive tooling
- ✓ Ability to run complex data analytics and implement further technological solutions more efficiently
- ✓ Lower operating costs

Larger banks have already formed strategic alliances with cloud providers, and all participants stated that at least some of their surveillance data will be hosted in the cloud. There remain some reservations regarding potential risks of reliance on third-party data management, including cyber security risk. Therefore, for about 50% of banks, the most sensitive personal data, such as HR data, may remain on premise, or within an internally hosted cloud network.

> **There are potential cost savings of up to 90% in data storage by moving to the cloud"**

5 The impact of technology

More than 90% of the banks interviewed said technology or data would represent the largest cost outlay for the surveillance function of the future; for most, it will be a combination of both. Respondents agreed that costs for acquiring skills and resources would reduce over time.

Figure 3: What do you anticipate will be largest expenditure for surveillance functions of the future?

5.1 Emerging technology in surveillance

Harnessing the power of machines to complement human intelligence

Artificial intelligence and machine learning will play a significant role in the shift away from analysts reviewing high volumes of alerts to a more intelligence-led approach within surveillance.

Reliance on simple rules and lexicon alerting mechanisms should reduce over time. However, based on banks' current experiences the regulatory expectation is that these methods will not be completely replaced. Consequently, lexicon alerting is expected to play a small but important role in the future to provide basic comfort over the most obvious risks.

Artificial intelligence and machine learning will enable calculation of risk scores for trades or communications, as well as aggregate risk scores for individuals. This will allow surveillance functions to prioritise their review to focus on higher risk alerts, as well as enabling problem areas to be detected earlier

> **"We all know lexicons do not work… in many ways you cannot solve today's problems with yesterday's solutions."**

> **"Currently, artificial intelligence and machine learning techniques, whilst proving highly successful in certain fields, tend to lack the ability to explain how they derive their results. There should be caution in blindly accepting answers just because the computer says so."**

5.1.1 Machine Learning

Dynamic threshold setting

Creating dynamic alert thresholds based on historical alert review outcomes will be a good first test for machine learning. This will enable surveillance models to better respond to dynamic market conditions, while maintaining focus on the cases with the highest risk and reducing the number of false positives. The result will be to automate some of the basic decision making in order to close large volumes of alerts which are processed by humans today, thereby increasing efficiency.

Reliability of dataset	— The ability to successfully deploy machine learning in surveillance will hinge on the reliability of a labelled data set. — Quality assurance over reviews, adequate governance and oversight, training and upskilling of review staff will be key factors in the short to medium term.
Regulatory scrutiny	— Banks will still need to demonstrate why a decision was made around an alert. — The ability to prove the accuracy and performance of the machine will be critical. — Robust testing techniques over a historical data set will be required to validate results.

5.1.2 Advancing technology in communications surveillance

Similarly, new technologies, such as Natural Language Processing and network analysis, will provide additional behavioural indicators which can be analysed by computer systems to generate a refined data set for manual review.

Natural language processing

This technology enables firms to programme computers to comprehend the underlying complexities of human language. For example, sentiment and context of discussion – in addition to the content of communications. Some of the advanced measures of natural language processing have been outlined in the table below:

Technology type	Definition
Voice transcription	— The ability to convert voice communications into text will, over time, allow for more cost-effective coverage of audio communications, potentially enabling banks to take advantage of more sophisticated analytics and technologies once audio is converted into text.
Entity extraction	— Extracting key information which is provided within communications into simplified pre-defined categories, which are computer readable and easily available for processing. This will facilitate the link between communications, trades and clients.
Sentiment analysis	— Process to analyse the meaning of language used in a context. This can be used to identify conversations exhibiting a behavioural marker for example, communications of secretive nature - “Don't want others in market to know”.
Topical analysis	— Summarising the subject matter of large volumes of communications in a unique set of key words to identify common topics of discussion across different segments of the population under surveillance.
Translation	— Converting text or words from one language into another whilst preserving the original meaning of the text or word. This will allow surveillance functions to expand geographical coverage of communications monitoring.

Network analysis

The ability to identify internal and external networks will be a powerful tool in future surveillance. Banks could monitor frequency of communications and intimacy of relationships. Mapping key network relationships could help identify and prioritise potential future risks.

5.2 Technology vendors

Levelling the playing field

Banks will have increased access to a wider range of vendors.

All the banks interviewed currently use at least one third-party technology provider in their surveillance programmes. 86% of banks interviewed anticipate the technology deployed within their surveillance functions in future will be a hybrid of vendor solutions and in-house developed models, however smaller banks are more likely to rely entirely on third-party vendors.

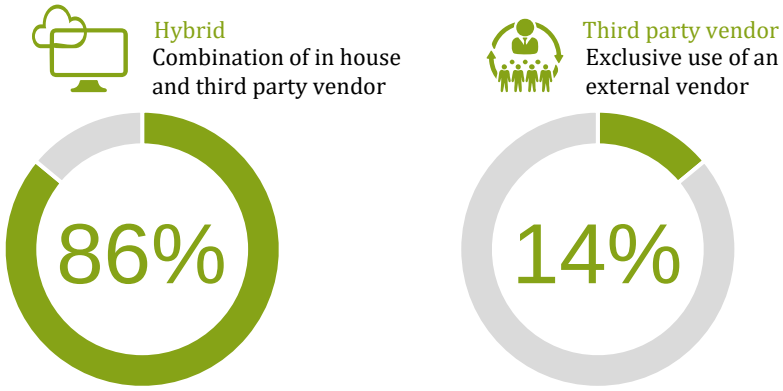


Figure 4: Who will build the surveillance technology of the future?

There is a commercial incentive for vendors and banks to create better surveillance solutions. As firms move away from expensive and inefficient existing legacy systems, vendors who develop surveillance solutions that use better quality data and deploy machine learning and artificial intelligence technology to enhance risk detection techniques will be in greater demand and find that they have a competitive advantage.

Firms with better surveillance systems will attract clients just as firms with better compliance and risk controls do. Firms with better data will be able to deploy this to clients' advantage in the giving of investment advice and in trading strategies.

5.3 Future technological challenges

Technology poses both an opportunity and a threat to surveillance.

Developments in technology will inevitably also create new challenges, particularly in the monitoring of communications.

Over the last decade, there has been a significant increase in use of social media and alternative communication channels, with this set to accelerate further amongst a new generation of traders. Surveillance functions will need to adapt accordingly and be conscious of developments in these areas, for example updates in popular messaging forums or new apps.

Banks will continue to need a robust policy around the use of personal devices and permitted communication channels and the ability to detect any unauthorised use may be prudent. With enhanced regulations around data protection coming into force globally, banks will continue to need to balance the requirement to monitor all communication channels used by employees from a risk perspective, with the need to protect their employees' personal data privacy.

6 What new skills will staff be required to have?

6.1 Smaller teams of experts

The impact of data and technological transformation will result in changes to the surveillance operating model and drive demand for new skills.

Current large process-driven, often offshore, review teams, many of which currently operate in high volume operations centres, are expected to transform into smaller centres of excellence comprising staff with specialist skills and knowledge. The expectation amongst over half of the banks interviewed is for surveillance processes to be performed onshore.

Figure 5: Where will surveillance processes be carried out in the future?

Surveillance teams will be expected to apply programming skills in order to analyse large data sets, thus, driving further automation of data processing. A surveillance data scientist community will emerge.

Subject matter focused experts will be integral to more investigative surveillance. These individuals will be expected to understand the risks, valuation and life cycle of products in a more tech-focussed climate. As algorithmic trading gains market share, surveillance teams will need to understand new and evolving market microstructure specific to the asset class and trading venues. The review process should involve fewer cases, but each case will be investigated more thoroughly.

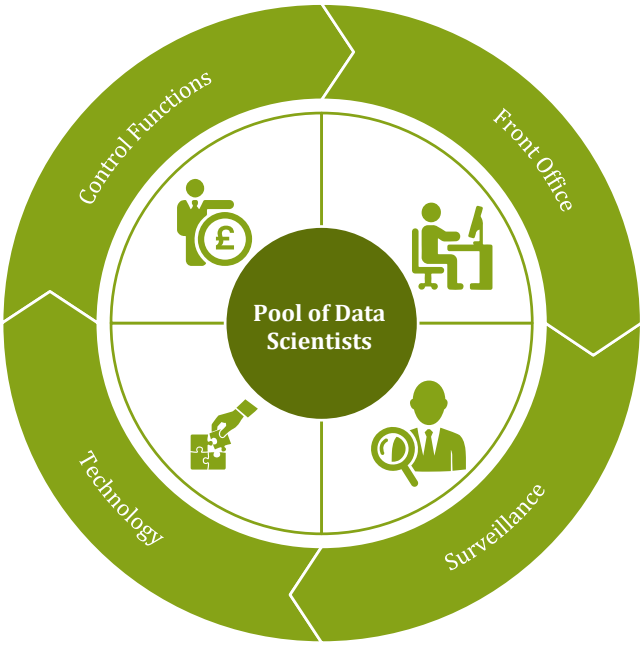
6.2 War for talent

The battle for skills is underway

Surveillance teams will need to compete with other functions of the bank for the same skillset. Front office, for example, will require people with similar skills to design and develop algorithmic trading strategies, and to help it leverage technology for commercial advantage.

Some banks are already pooling data science and analytics capabilities, drawing on the combined skillset for different projects across the bank and three lines of defence. Others will seek to employ a small team of data scientists to work solely on surveillance topics or gain access to these skills from the external market.

Whilst the strategy will vary based on the size and ambition of the surveillance operations, all banks interviewed have expressed an interest in acquiring these skills in the future.



7 Future-state operating model

The table below highlights the potential operating model of the future surveillance function compared to the current state. It explores the ways surveillance can partner with the business, as well as facilitate the convergence of compliance monitoring silos.

Current	Future
Data and Technology Procurement	
— The data required to undertake surveillance is fragmented and exists across several systems. These systems often sit downstream and are primarily owned by other functions including finance and operations. — There are limited synergies being realised in relation to the sharing of technology developments and data between surveillance and other functions, including front office. — Whilst surveillance is predominantly performed within the second line of defence, in a number of banks some capability has been deployed, or is in the process of being developed by the first line as well. — Third party vendor solutions, which apply rule-based detection models are being used by banks to perform communications and trade surveillance.	— Data will be sourced directly from front office trade capture systems. This will allow surveillance functions to benefit from increased granularity of data and will ensure data is complete, accurate and available in a timely manner. — Joint investment in technology between the front office, surveillance and other control functions without the development of separate and sometimes duplicate solutions, reducing the overall cost for the bank. — Investment into areas such as text and speech comprehension, network analysis and behavioural analytics will help perform more targeted risk-based surveillance.
Business Alignment and Insight Generation	
— Surveillance is often performed within the second line, with limited involvement or interaction with other areas of the business. — The review of initial alerts for communications and trade surveillance are typically performed by larger review teams, many of which are located near-shore or offshore, supported by a smaller number of trading experts. — Surveillance is primarily carried out to comply with regulatory requirements. There are limited business insights being generated by surveillance functions.	— Surveillance functions will better understand front office trading strategies and the associated inherent risks. Front office will share its knowledge about what is considered appropriate versus inappropriate behaviour in the context of an underlying product/market. This will be used to construct intelligent models to target market abuse and market misconduct. — There will be many opportunities for surveillance functions to demonstrate additional value. For example: – Analysis of topic modelling and associated trading patterns could be used to predict individual client demand, allowing banks to tailor products to particular clients. – As machines learn to better understand communications banks could generate more insight around interactions with clients, identifying sentiment and detecting client concerns at an earlier stage. — Whilst performing additional analysis, banks will also need to ensure they are not in breach of GDPR or any other data privacy requirements.

Current	Future
Organisational Structure	
— Trade and communications surveillance are performed as separate processes for the primary purpose of detecting market abuse. There is currently little synergy between these processes. — Control room and financial crime activities are run as separate processes, often by separate teams within the compliance function. This is driven by differences in the underlying data used within market abuse surveillance (e.g. trade and order data) and financial crime/control room activities (e.g. payments, entity information and insider lists). — Increasing expectations from some regulators that firms should consider the potential financial crime risk within their market abuse surveillance.[3]	— Opportunity to explore greater synergies between the operational and technological set up of communications and trade surveillance. — As data quality improves, technology advances and skillsets develop, many of these market abuse surveillance-led investments could also benefit and enhance the detection of financial crime. For example: – Leveraging product and market expertise within market abuse surveillance teams to detect money laundering risk within wholesale banking. – Using improved communications monitoring to gather context about transactions will complement existing transaction monitoring systems. – Network analysis technology will help to identify the potential end-customers in transactions and assist in customer due diligence and know-your-client processes. — Risk-weighted models will drive the identification of suspicious transactions in the context of financial crime.

Note: 3. Source: FCA Thematic Review TR19/4: Understanding the money laundering risks in the capital markets, June 2019

8 How can the industry collaborate better?

8.1 Creating an industry standard for surveillance

Banks could drive industry standards.

Collaboration across the banking industry could lead to the creation of research-based, scientifically verified models.

Many vendors offer solutions for trade surveillance in the marketplace which define and design alerts to mitigate market abuse risks. To varying degrees of sophistication, all banks have also invested in developing their own risk-specific detection models, running alongside vendor solutions. The question is whether by pooling this investment together, the industry could create academic research based, robust models in the future?

Working together, banks could apply lessons learned and promote 'industry standard' models for identifying different risk types, with potential to create robust models that could be applied across the industry. These models could drive efficiencies and greater consistency in the approach taken by banks.

Previously, this has worked well in the domain of financial risks, including market and credit risk, where there are many widely published industry-accepted models and calculation methodologies. As the regulation driving surveillance is principle-based, there is now an opportunity for the industry to collaborate and develop standardised models for the identification and measurement of non-financial market conduct risks, subject always to compliance with competition law.

8.2 The role of industry bodies, trading venues and regulators

Seeing the bigger picture

Banks are limited by the data that is available to them, as often it represents a narrow view of wider market activity. Trading venues and regulators, by contrast, have access to a much wider dataset, including quote, order, and execution metadata. Applying enhanced data analytics over this wide dataset would provide coverage over cross-product and cross-venue manipulation risks that banks cannot fully monitor for themselves.

All banks interviewed said they look forward to greater collaboration with regulators and industry bodies. Banks believe the industry could greatly benefit from the transfer of knowledge regarding good and bad practice observations, expectations of control frameworks and behaviours over time. This could be achieved through the following steps:

- Transfer of secondees between bank surveillance teams and the monitoring teams of regulators.
- Regulator-provided sandbox environments where anonymised test data sets and case studies are available for banks to stress test their systems against.

Case Study
June 2019

The Securities and Exchange Commission (SEC) charged five foreign traders from three different countries with engaging in circular trading[4]. The SEC's investigation leveraged the power of information available to venues and regulators and would have been almost impossible for a single bank to conduct in isolation.

> **"Geographical borders are relevant for regulators but not for surveillance"**

This would also provide a sense check for surveillance functions in assessing their own capabilities and promote greater harmonisation across the industry.

There is speculation as to whether there will be convergence or fragmentation of regulation in this space over the next five to ten years. One recommendation is for regulators to collaborate on a minimum global standard for surveillance that all jurisdictions will adhere to. Data privacy and data quality restrictions between geographical locations, may make collaboration difficult in the short to medium term. However, for banks that operate global surveillance programmes, this will be important in determining their long-term strategies.

Note: 4. Article 'SEC Freezes Assets in International Manipulative Trading Scheme'
Source: https://www.sec.gov/news/press-release/2019-101

8.3 Emergence of surveillance utilities

Should future surveillance be performed by an independent utility function?

Views are polarised as regards to using an independent utility function. Those supporting the function suggest it will lower operating costs for banks and promote standardisation of industry best practice while reducing the overall level of systemic risk.

Banks, however, remain sceptical about the practicalities of achieving this solution, particularly regarding the delegation of control, data harmonisation, data privacy and data security. A seismic change in perception, both in banks and regulators, would be necessary before a shared utility function could be a viable solution. Any such centralised utility would inevitably need to be regulated in order to maintain public trust. In practice, in the short to medium term, it seems unlikely that a utility function will form part of future state surveillance.

Case Study
July 2019

Six banks in the Nordic region announce the creation of a KYC utility[5], which centrally pools together Know Your Customer checks across large and medium commercial clients. The initiative is expected to help the banks in their efforts to crack down on money launderers.

Note: 5. Source: https://uk.reuters.com/article/us-europe-moneylaundering-nordics/nordic-banks-join-forces-to-combat-money-laundering-idUKKCN1U01MO

9 Next steps

9.1 Tactical recommendations

Secure consistency of organisational data for surveillance	— To ensure successful deployment of future solutions, banks should consider the compatibility and availability of data, actively engaging with the business and IT to identify the right data sources.
Ensure accurate labelling of data	— To ensure readiness to deploy machine learning and artificial intelligence, banks should review their current capability and accuracy of alert tagging. Accurate labelling of the data set is critical to ensure machine learning can be deployed effectively.
Restructure the organisation of data and people	— We cannot predict when there will be a truly integrated surveillance function at banks in the future, but as an initial step, banks can bring together different surveillance capabilities that currently exist in silos. For example, having analysts cover both trade and communications alerts for a particular asset class will facilitate a more investigative approach, as will ensuring intelligence can be shared more seamlessly between teams.
Invest to develop data-comfortable talent pool	— Surveillance functions can identify skillset shortages and begin to invest in their existing talent pool. For example, top talent can be recognised and trained to develop their data analytics and programming skills to enable better tuning of future surveillance models. This may result in the emergence of centres of excellence, where skills are aligned regionally based on the type of surveillance carried out.
Embed surveillance as a key commercial consideration	— Banks should consider incorporating surveillance as part of the new product approval process. This is to ensure current and future state surveillance continues to understand and capture the new and emerging product risks.
Embark on the regulatory journey	— Banks should start talking to their regulatory authorities about the evolving landscape of surveillance, particularly in the areas where there will be a shift in the technology approach (for example, the deployment of machine learning and artificial intelligence algorithms). The goal is to ensure all parties are proficient operators of this technology as well as the level of assurance to be provided.

9.2 Strategic considerations

Data and technology strategy	— Banks will need to assess whether they want to invest in building a common data layer across the bank, which brings all control function and business data together. — Banks will need to implement their chosen data management strategy, assessing whether all of the data will be hosted in the cloud, or whether there will be a combination of cloud and on premise solutions.
People strategy	— Banks may wish to partner with universities that offer courses that are aligned to data science skillsets. Collaboration with higher education facilities can promote work placements as part of an educational qualification. Targeted recruitment events would allow for future hires to be headhunted by surveillance functions. — First and second lines can work together to offer graduates the opportunity to experience working across multiple functions, making the overall experience agnostic to the function, but more tailored to the underlying skillset. — Banks can also build awareness of the developments amongst current staff, enabling them to upskill.
Commercial considerations	— Investment in surveillance could play a key role in safeguarding a bank's reputation which can enhance the level of trust and perception associated with a bank's brand. — Banks will promote confidence in financial markets. Customers may feel better protected which may increase the level of customer confidence in the fairness and accuracy of their transactions with a bank.

10 Glossary

Term	Definition
Algorithms	Set of defined instructions for making a calculation or to automate a decision-making process, widely used in the trading of financial instruments.
Artificial intelligence (AI)	Machine intelligence used to enhance, accelerate and automate decision making, simulating human intelligence.
Behavioural analytics	Method to detect the behaviours of individuals using computer-based systems to identify trends and patterns.
Cognitive tooling	Computer based tools used to assist and engage intellectual processing and critical thinking
Common data layer	A centrally sourced data structure used for storing and processing data that is accessible to multiple functions within an organisation.
Control room	The control room is primarily responsible for preserving the integrity of the firm's information barriers by monitoring and controlling the flow of confidential information between the firm's advisory side businesses (e.g. investment banking) and the public side (e.g. sales and trading).
Cross-functional data utility	Single data layer which can be accessed by different functions across an organisation.
False positive	An alert generated by surveillance processes as an indicator of high risk behaviour which upon investigation is determined to carry low or no risk.
First line of defence (1LOD)	Consists of the business owners, whose role is to identify risk, as well as execute actions to manage and mitigate these risks.
Front office	Revenue generating function within an investment bank that provides client services through sales and trading activities in the wholesale markets.
Indication of interest (IOI)	Expressing an interest in buying a security without entering into a formal agreement.
Lexicon	A set of key words and phrases typically used in the monitoring of electronic and audio communications to detect misconduct and market abuse.
Lexicon based model	Rules based model used to govern the surveillance of electronic and audio communications activities through keyword detection.
Machine learning	A component of artificial intelligence that allows systems to automate data analysis using algorithms. This allows a system to automatically learn and improve its own capability without being explicitly programmed to carry out specific tasks.
Natural language processing	Concerned with the interactions between computers and human languages, how to program computers to process and analyse large amounts of natural data in the same way as humans, through natural intelligence.
Offshore alert centre model	Operating model used by organisations to establish a team in a different geographical location. For surveillance, these teams typically perform a first level review of electronic and audio communications alerts, which are triggered by the lexicon-based model.
Rule based alerting systems	Applications / tools that can detect misconduct in electronic and audio communications through a set of defined rules or functions.
Second line of defence	Typically consists of compliance and risk functions, whose role is to set the standard for risk management through establishing policy and process to detect and mitigate risk.
Suspicious transaction and order report (STOR)	A process to report suspicious transactions where there are 'reasonable grounds' to suspect the transaction or order might constitute market abuse.
Trading venue	A trading venue is an official venue where financial instruments are traded by multiple third-party buyers and sellers.
Voice-to-text solutions	A computer-based process developed to enable the recognition and translation of a spoken language into text.

11 Key regulatory requirements

This table is for illustrative purposes and should not be deemed as a complete list of surveillance requirements.

Regulation Name	Region	Regulatory reference
Market Abuse Regulation	EMEA	Regulation (EU) No 596/2014 *MAR Article 16 Prevention and detection of market abuse* Commission Delegated Regulation (EU2016/ 957) *RTS 7 Appropriate arrangements, systems and procedures as well as notification templates to be used for preventing, detecting and reporting abusive practices or suspicious orders or transactions*
MiFID II	EMEA	COMMISSION DELEGATED REGULATION (EU) 2017/589 *Article 13 Automated surveillance system to detect market manipulation*
Securities Exchange Act of 1934	US	Section 3D (4B), Section 3D (13C)(iii), Section 6 (3I), Section 6 (3J), Section 6 (5A), Section 6 (5B), Section 15E (r)(2B), Section 15E (s)(1A)(iii), Section 17B (3)
MAS Bluebook	Singapore	Chapter 10 Section 2.3c, Chapter 10 Section 5.6, Chapter 10 Section 5.8
Australian Securities & Investments Commission	Australia	Chapter 5.11, Chapter 5A.5
Anti-Money Laundering directives	EMEA	DIRECTIVE (EU) 2015/849 Anti-money laundering directive paragraph 43, Article 12(e), Article 15(3), Article 18(2)

12 Contacts

AFME

James Kemp
Managing Director,
GFMA and AFME

Will Dennis
Managing Director,
Co-Head of Policy Division
will.dennis@afme.eu
+44 (0)20 3828 2683

Andrew Harvey
Managing Director Europe,
Global FX Division
aharvey@gfma.org
+44 (0)20 3828 2694

Richard Middleton
Managing Director,
Co-Head of Policy Division
richard.middleton@afme.eu
+44 (0)20 3828 2709

Louise Rodger
Director,
Compliance
Louise.Rodger@afme.eu
+44 (0)203828 2742

KPMG

Paul Tombleson
Partner, Risk Consulting
KPMG LLP
paul.tombleson@kpmg.co.uk
+44 (0)20 7311 3964

Lucas Ocelewicz
Director, Risk Consulting
KPMG LLP
lucas.ocelewicz@kpmg.co.uk
+44 (0)20 7311 5353

Rebecca Louden
Senior Manager, Risk Consulting
KPMG LLP
rebecca.louden@kpmg.co.uk
+ 44 (0)20 7311 3635

Dharam Shah
Senior Manager, Risk Consulting
KPMG LLP
dharam.shah@kpmg.co.uk
+44 (0)20 7311 6155

/ About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues.

We represent the leading global and European banks and other significant capital market players.

We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

We aim to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work.

Focus
on a wide range of market, business and prudential issues

Expertise
deep policy and technical skills

Strong relationships
with European and global policy makers

Breadth
broad global and European membership

Pan-European
organisation and perspective

Global reach
via the Global Financial Markets Association (GFMA)

London Office
39th Floor
25 Canada Square
London, E14 5LQ
United Kingdom
+44 (0)20 3828 2700

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium
+32 (0)2 788 3971

Frankfurt Office
Skyper Villa
Taunusanlage 1
60329 Frankfurt am Main
Germany
+49 (0)69 5050 60590

Press enquiries
Rebecca Hansford
Head of Media Relations
rebecca.hansford@afme.eu
+44 (0)20 3828 2693

Membership
Elena Travaglini
Head of Membership
elena.travaglini@afme.eu
+44 (0)20 3828 2733

Follow AFME on Twitter
@AFME_EU

AFME, 39th Floor, 25 Canada Square, London E14 5LQ, UK