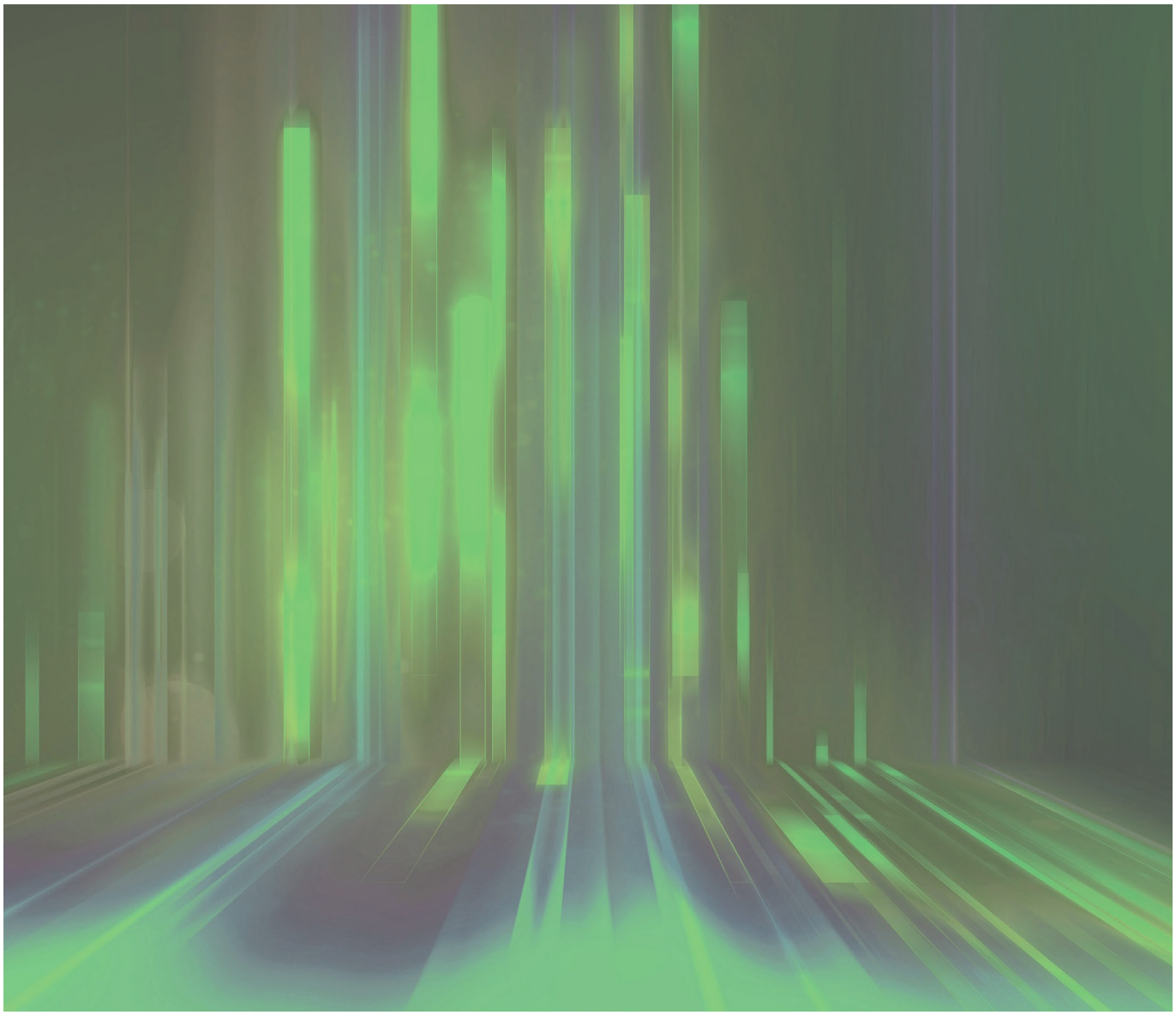
afme/
Finance for Europe

EY
Building a better working world

Governance of Market Abuse Surveillance Controls

An industry perspective

January 2021



Association for Financial Markets in Europe
www.afme.eu

Disclaimer

The Governance of Market Abuse Surveillance Controls (the "Report") is intended for general information only and is not intended to be and should not be relied upon as being legal, financial, investment, tax, regulatory business or other professional advice. AFME doesn't represent or warrant that the Report is accurate, suitable or complete and none of AFME, or its respective employees shall have any liability arising from, or relating to, the use of this Report or its contents.

Your receipt of this document is subject to paragraphs 3, 4, 5, 9, 10, 11 and 13 of the Terms of Use which are applicable to AFME's website (available at http://www.afme.eu/en/about-us/terms-conditions) and, for the purposes of such Terms of Use, this document shall be considered a "Material" (regardless of whether you have received or accessed it via AFME's website or otherwise).

AFME represents European wholesale firms and this paper is specifically targeted at its Members. Although much of what follows is relevant across the industry, global firms will have to take account of differences of local law and regulation, as well as the specifics of their unique business model, in planning and executing their surveillance governance strategy. This paper is not intended to be an exhaustive list of required changes and the key points covered in this paper may not apply to all firms.

January 2021

Contents

Foreword

AFME is pleased to publish "Governance of Market Abuse Surveillance Controls" in collaboration with EY.

In July 2016, the EU Market Abuse Regulation (MAR) came into effect, specifying the requirements for financial institutions to maintain necessary systems and controls intended to mitigate the risk of insider dealing, market manipulation and unlawful disclosure of inside information. Conduct failures in Libor and FX at the start of the decade heightened regulatory focus on firms' ability to effectively control the risks inherent in their business activities.

Over recent years there has been increased regulatory scrutiny over the application of the requirements in MAR. At the same time regulatory expectations have become more prescriptive, requiring firms to continuously assess the systems and controls that prevent, detect and report suspected market abuse.

The impact of the Covid-19 pandemic emphasised the importance of firms ensuring that their approaches continue to manage emerging risks caused by market volatility and changes to the working environment.

Since the 2008 financial crisis, regulators globally have determined to hold senior managers and executives within financial services firms individually accountable for the management of risks and compliance with regulations. Understanding what good governance over the control of market abuse risks looks like and implementing the requisite processes to manage this, is critical for senior managers. Firms may have taken different approaches in developing their surveillance governance structures, but all share the same goal of ensuring an appropriate level of 1st line of defence (1LoD) and 2nd line of defence (2LoD) oversight.

The surveillance control environment is now at an inflection point, with regulators expecting more agility in the post-pandemic environment and firms recognising the benefits of a more operationally efficient and cost-effective model with more insightful outcomes.

With that context in mind, this paper discusses the key developments and challenges facing surveillance teams and senior management, drawing on survey responses and deep dive interviews with AFME members and European regulators. We hope that the insights in this paper will help to frame the key aspects of this debate and provide firms with industry insight to advance the effectiveness of their surveillance governance.

AFME would like to thank EY for their support in the production of this report, as well as Members from AFME's Surveillance Working Group and Compliance Committee, all of whom made contributions that were integral to the development of this publication. We are grateful to all those who have participated in this paper, including Member firms and European regulators.

This paper complements AFME and EY's report on "The Future of the Compliance Control Environment[1]", published in November 2020.

James Kemp
Managing Director
GFMA and AFME

[1] The Future of the Compliance Control Environment is available at: www.afme.eu/reports/publications/details/The-Future-of-the-Compliance-Control-Environment

Executive Summary

This report was commissioned to reflect common discussion points regarding the current state of surveillance governance, as well as the direction of travel and key questions AFME members are considering as they formulate their future strategic roadmap. The observations presented in this paper are based on a structured survey completed by 18 AFME members, 8 further deep dive interviews conducted with AFME members, 2 interviews with regulatory bodies and EYs own experience supporting firms to develop effective surveillance controls. As part of this approach, a conscious effort was made to engage with firms of different sizes across European jurisdictions, to ensure the paper is representative of the diverse AFME membership.

Based on members' feedback, financial institutions have taken different approaches to establishing and maintaining 'good governance' over their surveillance control frameworks. It is clear that schools of thought are entering a new phase of development in line with the evolution of surveillance as a function. As we enter this next generation of surveillance, firms, vendors and regulatory bodies will all have a part to play in defining and establishing a target vision.

Establishing effective surveillance requires a multi-faceted approach: Teams must be clearly structured to align skills and provide delineation of tasks through an operating model. Processes must be designed, documented and implemented both pre- and post-submission of a suspicious transaction & order report (STOR). A framework of supporting processes is also needed to support and govern the STOR process. Traders, booking models and data sources must be mapped to understand completeness of coverage. If firms are able to critically assess their own strategy across each of these five areas, then they will be well positioned to manage their market abuse risks over the next five years:

1

Restructuring the operating model…

There is a strong desire for change in the structure of surveillance teams amongst financial institutions. The legacy setup of distinct trade, e-comms and voice surveillance teams is being re-considered, with 2 AFME members interviewed already moving to an integrated, cross-channel team organised by asset class and/or business line. These firms are recognising immediate benefits in the effectiveness of investigations and it is likely that many more firms will follow suit. 'Holistic' surveillance with a single platform generating entity-centric alerts across trade and communication data sources may still feel some way off, however the integration of people and process is beginning and delivering value.

2

Navigating risks through the STOR process…

Following a robust, well-governed and well-documented process from the inception of an alert through to conclusion has become paramount to ensuring a consistent outcome. The threshold of reasonable suspicion is one that requires judgement, and the risks of under-reporting, over-reporting and late reporting are real. Clear corporate definitions and processes are needed to manage these risks, along with proactive dialogue with regulators when needed. A common discussion point amongst interview participants was the extent to which a firm should continue to investigate a potential instance of market abuse after submitting a STOR to the regulator. Judgement over the extent and type of further investigation warranted is predominantly made on a case-by-case basis and will often differ depending on whether the STOR was related to client or own firm behaviour. There is clearly a balance to be struck between investigating further and reducing the risk of facilitating future market abuse, versus avoiding the risk of 'tipping off' and prejudicing a regulatory investigation.

3

Establishing a well-governed surveillance framework…

In order to accelerate the surveillance roadmap whilst sustainably managing risks and staying compliant, surveillance tools and scenarios must be supported by a robust framework approach aligned to the surveillance strategy. In order to do this, firms need a mature risk assessment process, insightful MI and an integrated set of processes to continually refine and calibrate controls in response to constantly changing risk profiles. The key elements in meeting expectations are the robustness of the governance and oversight framework and the extent to

which management respond to surveillance findings and use them to inform their forward-looking controls strategy. Change must be a business-as-usual process if compliance is to become sustainable.

4 **Chasing completeness…**

Surveillance has continued to develop since the introduction of MAR in 2016, coverage has vastly increased across products and data and regulatory expectations have evolved in line with this. However, firms still face challenges in ensuring completeness across trades, orders, quotes and communications. External data quality is a challenge that the industry must address in concert to make venue completeness a sustainable objective. Ultimately completeness cannot be assumed and 'completeness assessments' are becoming a core component to help self-identify emerging data or business gaps in the control coverage. This ongoing self-assessment and enhancement process in line with the evolution of the business itself is now an expected part of an effective overall framework. As firms continue to chase completeness the question is being asked over whether this dedication of effort is congruent with a risk-based approach and focus is now shifting to effectiveness.

5 **A change in approach: focusing on risk driven methodologies…**

With a robust framework established and confidence in coverage, firms at the leading edge of surveillance are now looking to tackle the effectiveness challenge. Investigatory analytics and non-alert driven data-centric reviews are two areas where firms have expressed a desire to see advancements. These new targeted techniques can supersede less efficient legacy approaches that helped create industry 'good' practice which is now perceived to lack insightful value. Innovation in surveillance techniques does not necessarily require new technology, but rather an agreed industry approach to measuring effectiveness that will allow firms to migrate away from resource intensive and inefficient tick-box engines and instead evolve risk-focused approaches.

A force for change…

The need for further enhancements in the governance of surveillance is clear, however maintaining this can be a moving target as regulatory expectations, technological capabilities and what is considered good practice continue to shift. AFME member feedback suggests that surveillance is now in a transition state with firms seeking more effective and cost-efficient methods; and therefore, governance over processes, systems and controls will need to evolve accordingly. In response to this, firms are proactively considering the strategic future state for effective governance. If firms continue to ask critical questions of their strategic roadmap against the themes outlined above, they will be in a better position to achieve 'good governance', allowing senior managers and regulators alike to have confidence in the ongoing effectiveness of a robust and dynamic surveillance framework.

Restructuring the Operating Model

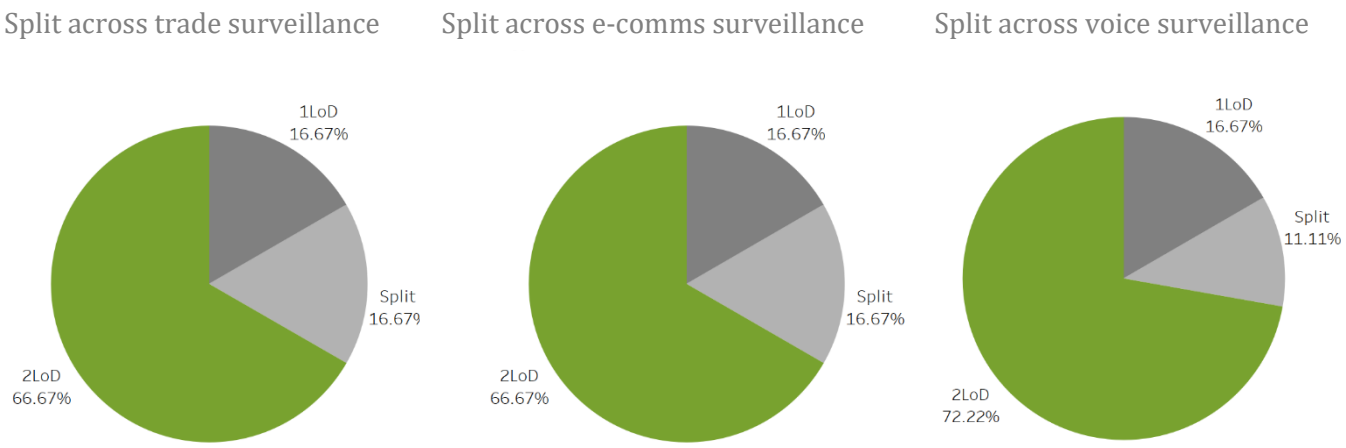
Traditionally surveillance has been an activity completed to comply with regulation and hence has been the sole remit of compliance. Over the last decade we've seen the emergence and growth of 1st line control teams who, in many cases have taken on responsibility for designing and operating a number of market abuse controls, sometimes including surveillance. Whilst there are benefits and challenges with both approaches, the consensus suggests that market abuse surveillance is predominantly a 2LoD role.

Some firms have considered merging market abuse surveillance teams with the broader financial crime teams, although convergence with AML transaction monitoring of markets trades appears to be some way off for now. In some instances, firms have merged their unauthorised trading monitoring (an internal fraud against the bank rather than an abuse against the market) into the surveillance analysts' role.

Current Operating Model and Lines of Defence

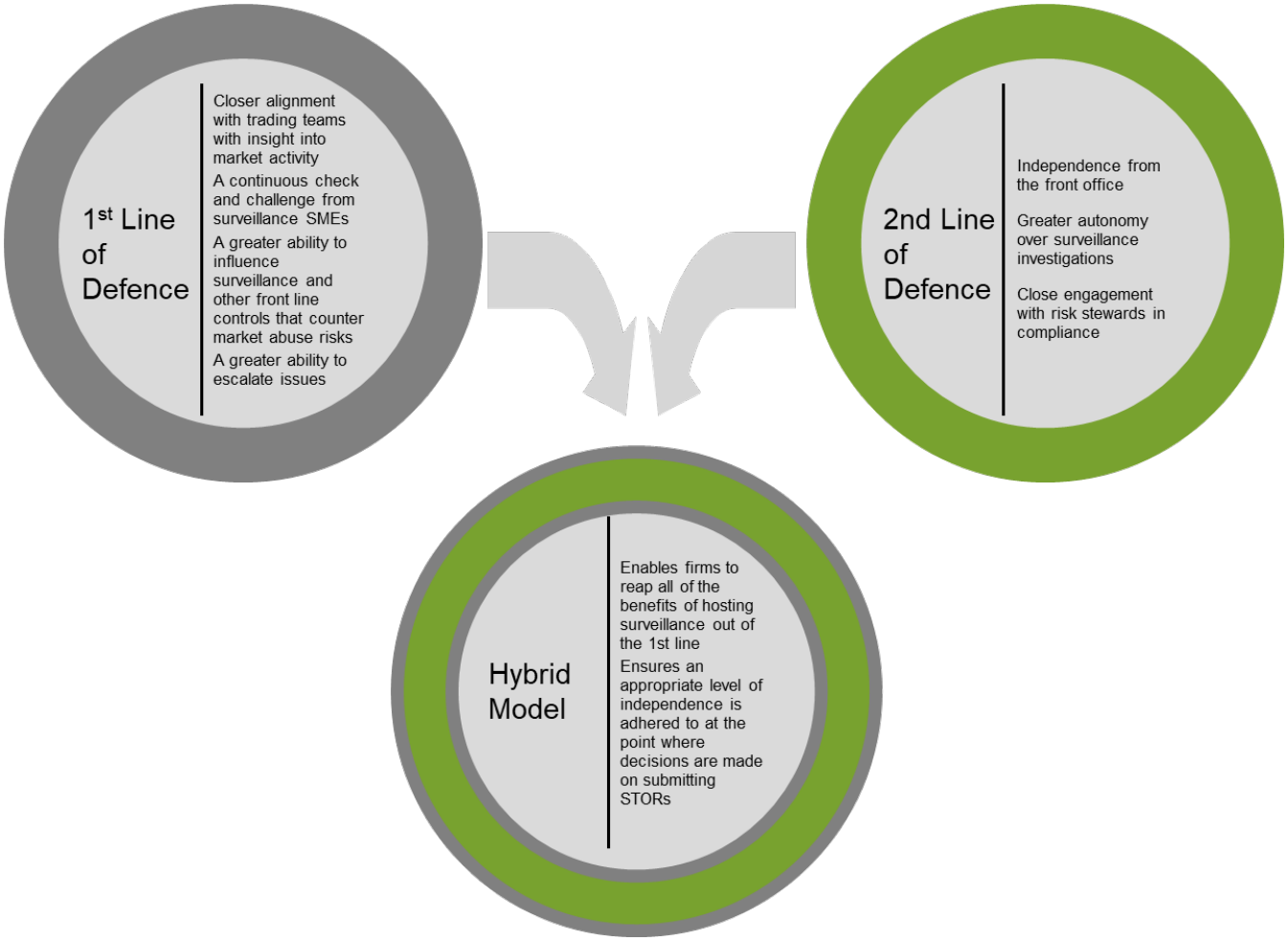
The majority of European firms operate surveillance from the 2nd line of defence. Industry debate has discussed this topic over the past few years and whilst a small number of firms have moved their surveillance teams into the 1st line of defence, typically within a 1LoD "Controls" team (also referred to as "line 1.5"), this remains less typical. The majority of firms operate both trade[2] surveillance and communications surveillance, both e-comms and voice, from the same line of defence, although there are some exceptions to this.

Figure 1.1: Split of Trade, e-comms and V-comms across Lines of Defence:



[2] 'Trade surveillance' is used here and throughout with a broad definition which encompasses the surveillance of trades, orders and quotes.

Figure 1.2: Benefits of operating surveillance in 1LoD, 2LoD and Hybrid model:



Integrated surveillance

The "holistic" surveillance structure as a concept faced high expectations but has not yet proven to be a practically achievable alternative to the status quo. In its original context, holistic surveillance was often referred to as a single alerting system generating alerts using scenarios that span trade, e-comms and voice data. Whilst some vendors and firms have made limited progress towards this, many firms continue to hold a more pragmatic shorter-term vision for greater integration of trade, e-comms and voice surveillance at a post- alert stage, i.e., during the review and investigation process.

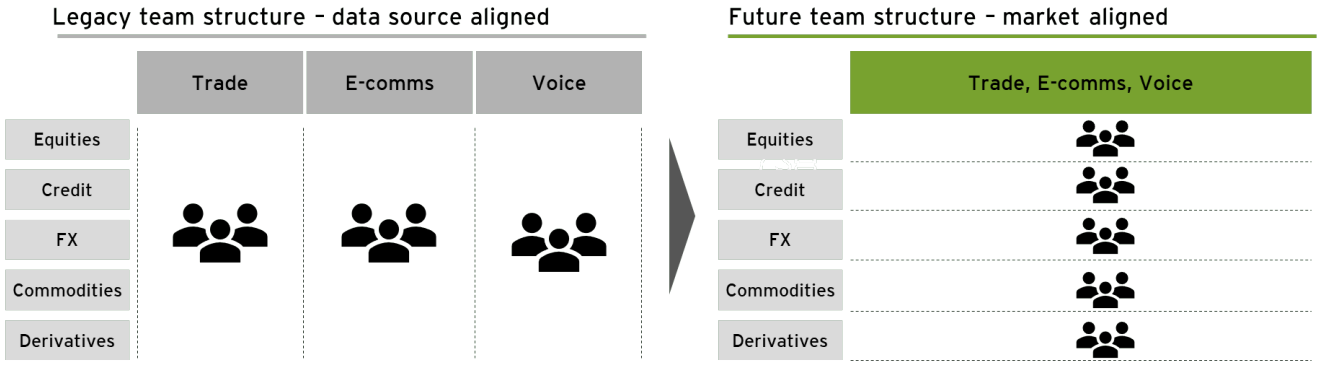
Typical review processes for alerts from the distinct trade, e-comms or voice alerting systems will each enable access to data from other media, e.g. trade surveillance alert reviewers will have access to the archive of communications data, though querying these vast and complex datasets often spanning multiple front office or source systems to find information specific and relevant to the investigation can be challenging and inefficient to the extent that it can prove impractical other than on an exception basis. Review teams do however currently continue to typically be divided into separate units focusing separately on trade, e-comms and voice reviews. This division is driven by several factors including legacy operating models that can involve a spread of resource across geographies, disparate data types, separate systems and differing scope (market abuse vs broader conduct risks) often driven by the specific requirements of internal stakeholder groups.

The direction of travel for the industry remains towards greater integration across surveillance channels. As firms are looking at the operating model and processes to achieve this, many are looking at re-structuring their teams so that personnel are aligned by asset class, market, or by business unit, agnostic of the data or platform that originated the alert. Pragmatic hurdles to overcome this involve providing access to a wider

range of tooling; providing cross-system case management (including integration with underlying detection systems); and developing new processes to manage alert volume spikes. For large firms where legacy comms or trade specific surveillance teams can be extensive and have been established across multiple geographies, disrupting this model can provide a significant challenge and potentially increase risk. Firms that can address these challenges will be able to move towards a more practical integration of surveillance supported by analysts with greater insight and context around the issues they are reviewing whilst avoiding the expectations that" holistic" surveillance set, at least in the medium term.

Whilst moving to an integrated product-centric appears to have many benefits, one challenge that can arise from this model is covering cross-product risks, which require connectivity across the product- centric teams.

Figure 1.3: Movement from data-source aligned legacy team structure to a more market aligned future team structure:

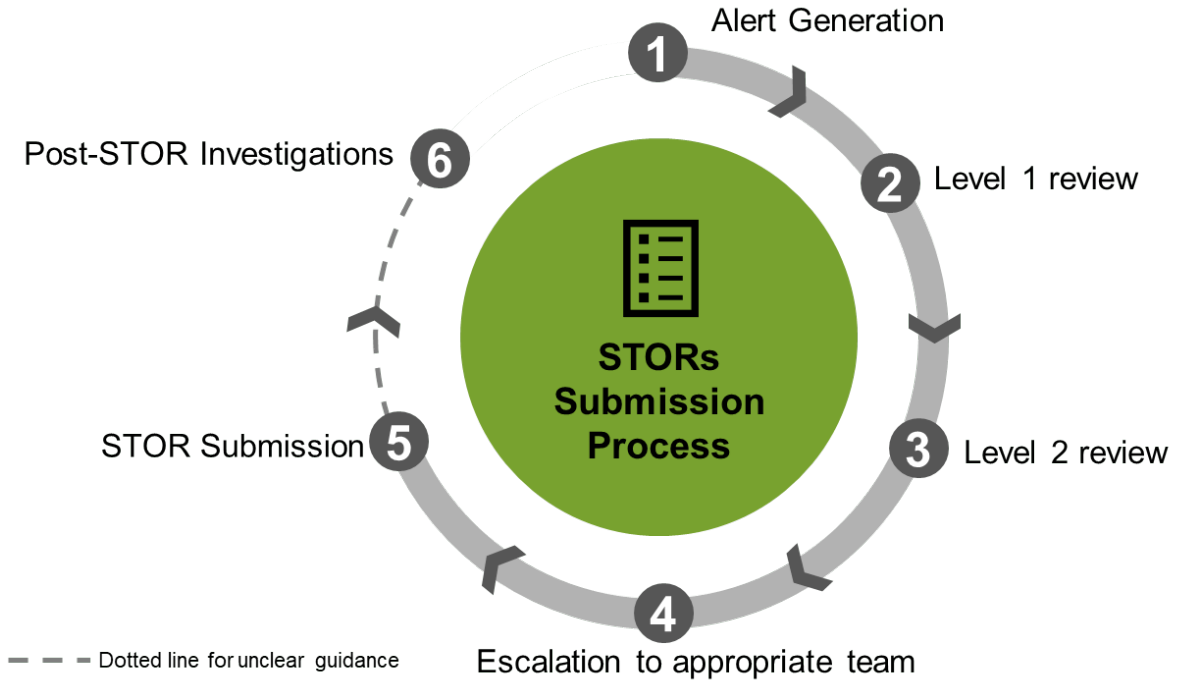


Navigating risks through the STOR process

53% of survey responders pragmatically consider timely submission of the STOR report to be within 14 days or less of a trade

As a result of the Senior Managers and Certification regime ("SMCR") and an increasing focus on the conduct agenda, senior managers across the financial services industry are now more acutely aware of the risks that they are responsible for controlling, including market abuse risk. This has, in some cases, resulted in a number of additional senior parties across the 1st and 2nd lines of defence being consulted before potential STOR submissions are made to the regulator. The need to have more senior management awareness, has for many of the AFME members interviewed, created additional layers of sign-off and oversight in the STOR submission process, potentially slowing down the escalation process and reducing the number of STORs that are raised. It is also important for firms to factor in and mitigate any possible conflict of interest where 1st line senior management is consulted prior to a STOR submission.

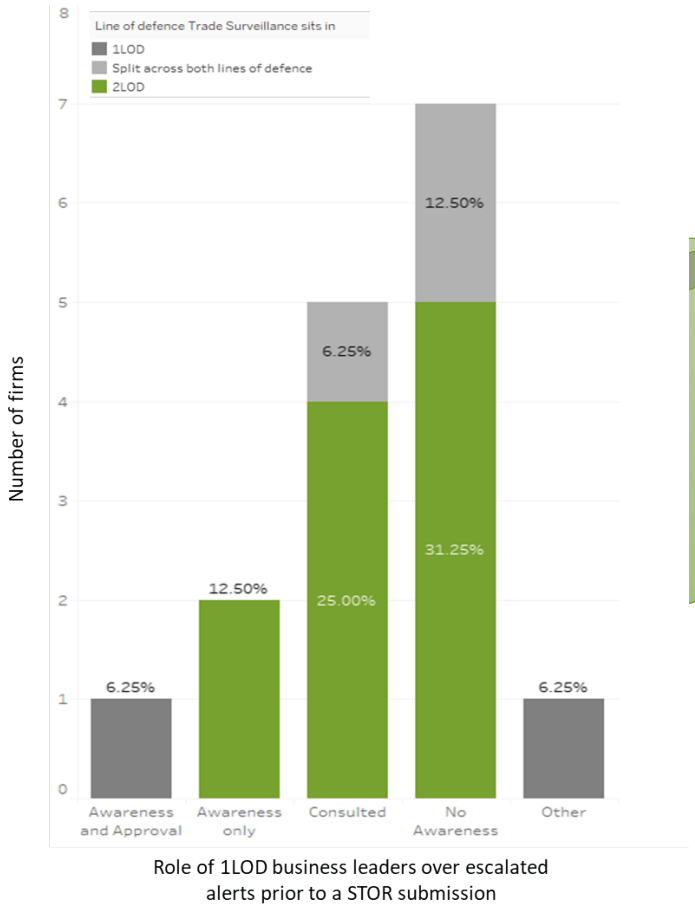
Figure 2.1: STOR submission process:



Initial alert review / triage

Surveillance systems and processes typically generate a number of alerts or, commonly in the instances of manual trade surveillance and voice surveillance, a level of sample reviews required. Alerts are then investigated, often escalated through several levels of review, and either closed as not suspicious or raised as a STOR. For most firms, the submission of a STOR will, at a minimum, require approval from someone independent of the key reviewer. Typically, the approvers for STORs are the Head of Compliance or Head of Surveillance although for some firms, approval may be necessary from a risk owner in the 1st line (such as a head of a business line) or their formal delegate (often sitting in the control function).

Figure 2.2: Role of 1LoD business leaders over escalations prior to STOR submissions:



- *Around 44% of firms suggested that their 1LoD Heads have 'No Awareness' when it comes to their role over escalated alerts prior to STOR submissions*
- *Around 31% of firms suggested that their 1LoD Heads are 'Consulted' for escalated alerts prior to STOR submissions*

Alert review supervision and quality control

Formalised ongoing quality control sampling as a concept was relatively unheard of a few years ago but is now commonplace amongst most firms. Sample volumes vary, with some firms performing secondary quality reviews on as few as 1% of alert reviews whilst others will undertake sampling of 10% or more. An aggregate average sample size of around 5% is typical. More mature quality control processes have developed methodologies that allow the sampling to be increased in areas of greater risk and reduced in areas of lower risk. Sampling also provides a simple lever to adjust in response to a changing risk environment. In the market turbulence and changing risk environment witnessed during 2020, quality control has been used to scale up and down the level of control deployed in response to perceived moves in inherent risk.

There is some industry challenge on the value of quality control sampling. Using quality control to identify procedural deviations or documentation lapses is useful but more valuable is validation of judgements reached which requires quality control analysts to have a skill and experience on a par with or exceeding that of surveillance analysts. Whilst "smoking gun" tests, which insert test cases of market abuse activity into live surveillance systems to check analyst detection, are uncommon, typically due to concerns around false alarms, some of the Heads of Surveillance we interviewed suggested that their use may become more commonplace in future.

Defining reasonable suspicion

The expectation set by regulatory bodies is that firms should submit a STOR where there is 'reasonable suspicion' that market abuse activity has occurred either by a client or internally. However, the point at which an investigation can evidence 'reasonable suspicion', and therefore ultimately engage in the submission of a STOR, is a highly debated topic. AFME members raised 2 clear approaches to determining where the line should be drawn when defining 'reasonable suspicion':

1) **Detailed submission:**

The first approach recognises that a relatively granular level of detail is required in order to complete the STOR template provided by regulators. Some firms explained that in order to meet the definition of 'reasonable suspicion' they had to have reached the later stages of the investigation process before being able to file a STOR. Existing challenges relating to access to data and the complexity of different systems, suggest that getting to this level of detail goes beyond demonstrating 'reasonable suspicion' and can hinder a firm's ability to submit suspicious activity in a timely fashion.

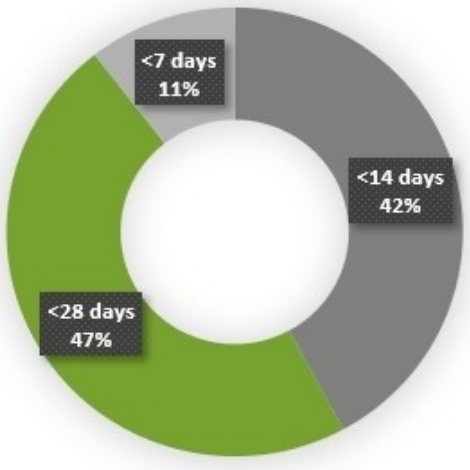
AFME Member: "I would still maintain that the bar for a STOR submission is really high"

2) **Earliest opportunity:**

The second approach is where firms submit STORs during the earlier stages of an investigation, meaning that some of the information included in the STOR may be at a higher level of detail than the template requests. Some AFME members interviewed suggested that they were more comfortable when setting a lower bar for 'reasonable suspicion', as they are able to communicate information on escalated investigations in a timelier fashion and then maintain continuous dialogue with the regulator as more evidence is collected and made available. However, one perceived negative aspect this approach is that there is a higher chance that some STORs are submitted before evidence is brought to light that adequately explains the behaviour. It also increases the potential for over-reporting that may detract focus from higher risk and more meaningful submissions.

With both approaches the key principle to be adhered to is to submit as soon as reasonable suspicion is formed. Having a clear process to determine when a corporate definition of 'reasonable suspicion' is met and to then report immediately is key. Whilst some firms would like to see more formal guidance to help define 'reasonable suspicion', there will inevitably always be nuances to cases. For example, it can be argued that the bar for 'reasonable suspicion' is different for market manipulation activity vs insider dealing, given evidencing for market manipulation may be solely based on transactional activity whereas insider dealing will often require information beyond this to fully evidence a case. Regulators recognise that cases can be complex and forming a clear picture can take time but the relationship with the regulator, as with any relationship, benefits from strong communication. Some firms will communicate with the regulator through the STOR report and in other cases will do so after the STOR report, either way this communication can be a useful mechanism to use in complex situations or where there is any doubt.

Figure 2.3: Timeframe that firms pragmatically consider as timely submission of the STOR:



Report submission

Having a clear STOR process

Having a clear process for escalation and ultimately STOR submission is important.

Figure 2.4: Areas where firms without a clear process may experience delays or challenge:

Submitting STORs can challenge organisations ability to take timely, collective decisions confirming that the threshold of 'reasonable suspicion' has been met. In some instances, firms will have to consider submitting STORs on employees or long-term clients which can place greater importance on having a clear process to manage potentially conflicting interests and allow themselves to come to a collective decision within a short timeframe.

Figure 2.5: What firms should document during the STOR submission process:

Firms should seek to ensure that their alert escalation and STOR submission process is well-documented and includes:	Who should be informed and consulted pre-submission, with clear guidance that outside of the defined escalation process information should only be shared on a need-to-know basis
	Who should approve the STOR submission
	Steps to be taken pre-submission
	Guidance on how to determine whether the level of suspicion necessary for a STOR submission has been met
	Guidance on what processes to follow after the STOR has been submitted. This may differ where the STOR relates to the behaviour of an employee, a client or other external market participants

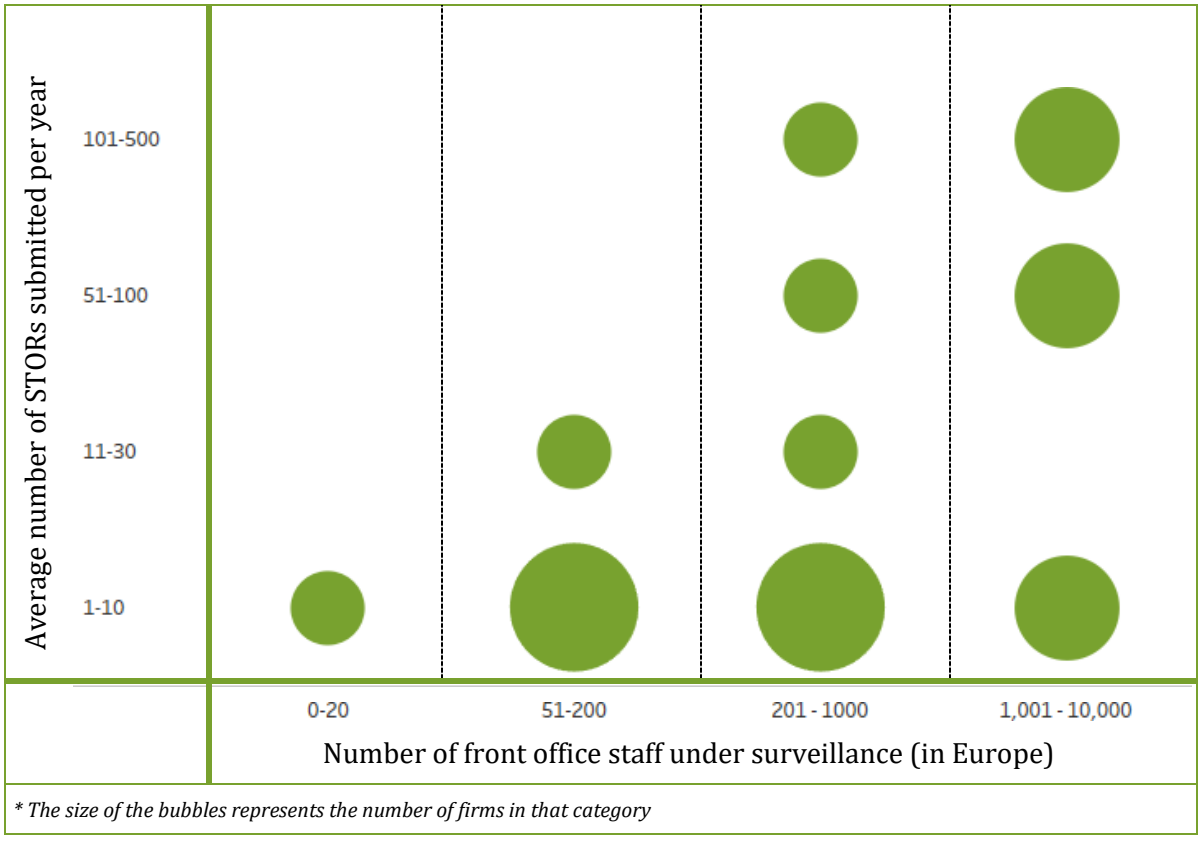
Balancing risks post-STOR submission

The process to be followed after a STOR has been submitted is often less well understood than the process for creating a STOR. Some regulators take the view that a single firm will only ever have a suspicion of market abuse and may never be able to determine with any certainty whether it has occurred. Some regulatory guidance goes further to highlight to firms the risk of disrupting a regulatory investigation by continuing an in-house investigation. However, other regulatory guidance obliges firms to act where they identify a risk that

market abuse is continuing to occur, for example where multiple suspicions have been raised, in order to reduce the risk that abusive activity continues to occur. This leaves firms balancing post-STOR risks of, on the one hand, over-acting and potentially compromising a regulatory investigation, and on the other hand, under-acting and continuing to facilitate ongoing abuse of the market. Most firms report that, without further guidance on post-STOR processes, finding the right balance here is currently done on a 'case-by-case' basis.

One area requiring further improvements is the ongoing monitoring, or enhanced monitoring, of clients for whom a STOR has been submitted or a 'near-miss' has been identified. There will inevitably be cases where there is some suspicion but not reasonable suspicion. For example, a single, likely-lucrative, trade ahead of an event-driven market price move without any further evidence may be unlikely to result in a STOR but a pattern of this activity or further evidence, such as a link to an issuer, which may come days or weeks later, may then cause the initial activity to be reconsidered. For all but the smallest of firms, human memory alone is unlikely to suffice in storing and retrieving these parcels of intelligence of relevance to future alerts; some in the industry would like to see greater use of systems or processes to log clients that have had STORs raised or near-misses (or perhaps a lower grade of suspicion) that allow the automated retrieval and flagging of this intelligence to investigators alongside future alerts. Guidance is clear that understanding the risk that clients pose is important and whilst some of this may be static KYC (know-your-customer) and onboarding information, we may see more dynamic customer risk assessment data become a standard input for the next generation of surveillance systems.

Figure 2.6: Number of front office staff under surveillance vs. Average number of STORs submitted per year:



** The size of the bubbles represents the number of firms in that category*

Governance over non-reporting

Governance over the STOR submission process is a highly discussed area; however, some firms have called out the easily overlooked but equally important governance processes followed when an investigation does not result in the submission of STOR. It is imperative that firms are comprehensive in their record keeping of evidence supporting decisions to close an investigation before it reaches the point of a submission, whether that be at first review or for alerts that have been escalated and investigated but found to be 'near-misses'.

In the UK firms also have the option of submitting a market observation (MO) rather than a STOR. However, four firms interviewed cited that regulatory guidance is not clear in determining when it is appropriate to

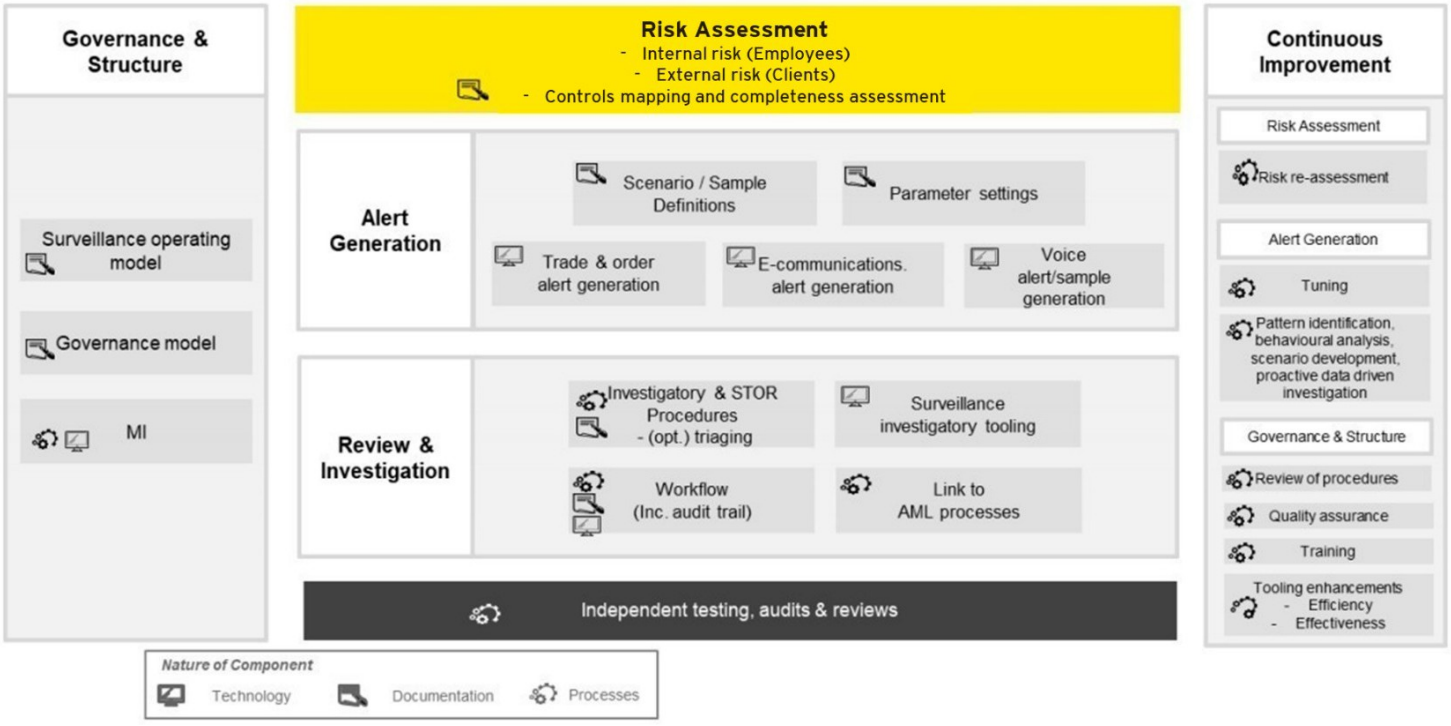
submit a MO vs a STOR. In some instances, we have observed firms submitting MOs where they are not directly involved in the activity in question. However, two AFME members interviewed use MOs as a way to open a dialogue with the regulator around an investigation, before all the necessary evidence has been gathered that may result in the submission of a STOR. With this in mind firms are asking whether the bar for suspicion should be lower for an MO than a STOR to promote early communication of suspicious activity.

In general, firms interviewed saw value in the creation of the market observation option and, whilst further guidance on the reporting boundaries may drive greater clarity and consistency, firms would be keen to see the MO concept adopted more widely across Europe.

Control management

Ensuring a proportionate and robust set of surveillance controls that apply current good practice across all aspects of surveillance is a constant challenge for surveillance teams. Given the 'black swan' type problem that detection of market abuse events occurs proving efficacy can be difficult or impossible to achieve (at least not within practical timescales) through statistical analysis. Therefore, firms are generally reliant upon a qualitative assessment of their control framework alone. Less mature surveillance teams may look simplistically at the scenarios deployed against those articulated through regulation to assess their compliance. However more mature surveillance teams will look at the components of their surveillance control framework. Assessing detective scenarios against the self-identified higher residual risks from the risk assessment is an important element of this, however the extent to which these scenarios can be relied upon to mitigate risks is dependent upon the rest of the framework: including management information (MI), calibration, investigatory processes and training. Development of clear standards across this framework and well-established processes to implement these is the method now used to validate control efficacy. One Head of Surveillance commented during interviews in Q4 2020, that "surveillance is still maturing

Figure 3.1: EY's Surveillance Framework:



Two tools that firms use to ensure their surveillance controls are proportionate are the risk assessment and independent reviews

Risk assessment

Market abuse risk assessments have become standard practice, in line with regulatory guidance. Whilst these remain a regulatory expectation predominantly in Europe, many global firms have incorporated these worldwide as part of their view of global standards for operating effective surveillance. Simple assessments may focus on surveillance controls whilst more mature assessments will consider the broader non-surveillance controls in place against the risks, enabling firms to identify changes needed to both surveillance and non-surveillance controls to manage high residual risks. Most firms conduct their risk assessment refresh on an annual basis, while some may refresh more frequently.

Taking a risk-based approach: more than a risk assessment

Risk assessments are the first step that allow firms to understand their risk profile. The decision over whether to undertake a market abuse specific risk assessment is straightforward, however the options of how to respond to the risk assessment are more varied. The natural output of a risk assessment is a matrix of residual risks across market abuse scenarios integrated into business lines and products. While some risk assessments will produce a binary result, many firms now produce a more variable view of residual risk from low to high. In responding to this some firms will focus automated scenarios only on higher rated risks whilst other firms will opt for completeness of scenario coverage with enhanced procedures or risk-based tuning that allows efforts to be focus on areas of higher risk. Risk assessments identify gaps that need closing and provide a useful articulation of the enhancements required for surveillance teams, but beyond the binary gaps there is not yet convergence across the industry on how to apply a consistent 'risk-based' approach in practice.

MI: the continuous risk assessment

The presentation of Management Information ('MI') has come under increased scrutiny as risk owners are being asked how they practically own the risk and senior managers are being asked how they govern the controls and maintain a constant understanding of risk and control effectiveness. Whilst traditional MI focused on operational metrics, such as alert volumes, more advanced MI is now providing senior managers with greater insight into market activity and potential risks. Some firms now have alert trending, risk assessment overlays and metrics on underlying business activity within their MI that help senior managers to provide oversight over not just the surveillance control operation but also the ongoing view of market abuse risk inherent within the business activity. Critical to making MI successful is having a clear agreement between the MI receiver and the MI producer on the purpose and need that the MI is addressing. Clarity of purpose should help to drive more targeted data points and actionable results. As risk assessments are becoming more data driven and MI is become more risk-focused a few firms expect that the purpose of the risk assessment and MI may begin to converge.

- *All survey respondents suggested that 'Alert Volumes' are MI metrics used for governance oversight of e-comms*
- *92% of survey respondents also use 'Escalation false/positive rates' for oversight of e-comms*
- *25% of survey respondents suggested that they have no MI metrics for over voice surveillance*

Independent reviews

Internal check and challenge over surveillance controls is one of the key measures employed over the surveillance framework to assess its adequacy. For the minority of firms operating surveillance out of the 1LoD the check and challenge can be given by 2LoD Compliance Advisory teams. For those operating surveillance out of the 2LoD, their sister team 2LoD Compliance Advisory will provide advice but its independence is compromised. For both operating models, a level of reliance is placed upon 3rd Line of Defence (3LoD) as the final internal check that the framework has been designed and is operating effectively.

Internal audit reviews conducted by 3LoD can be useful to provide an independent view, escalate issues for attention, increase support within the firm and demonstrate regulatory obligations to review the controls have been met. However, internal auditors will cover many areas, with surveillance being just one, and so are rarely specialised on the topic and familiar with the various regulatory requirements, industry guidance and common standards that continuously evolve around surveillance. Therefore, internal audits may focus on more generic control standards and at times focus attention in the wrong areas. Their objective is often also to identify gaps in regulatory adherence rather than the management of market abuse risk. Whilst in theory the two are identical, in reality the latter is more nuanced and driven by less well-defined criteria; this can result in a tendency to drive prioritisation around individual gaps, for example product and scenario gaps, and put less emphasis on aggregated risks, such as meeting global standards, that may be more impactful.

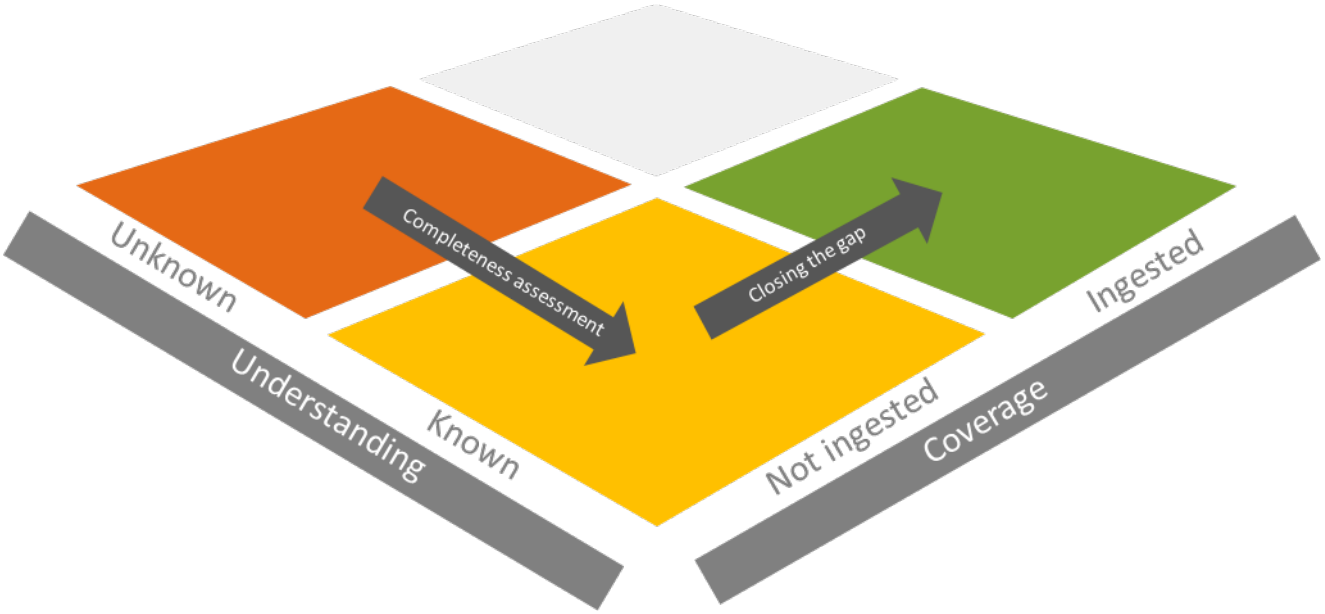
Given the progress of regulatory focus on surveillance, internal audits are increasingly regular and commonplace. For some firms the volume of separate audits is rising, each covering a slightly different scope but many asking similar questions. One firm reported that they had experienced around 100 separate internal audits within 12 months. Cross-skilling within the audit teams is important to avoid duplication and avoid audits consuming significant time from surveillance teams, repeatedly explaining surveillance concepts to multiple different auditors.

Some firms, particularly those with Surveillance in 2LoD who do not have the benefit of a continuous 2nd line check and challenge, would like to see a 3LoD move away from the multitude of point in time audits and towards a continuous audit model. This allows check and challenge at every stage, enables the auditors to become more familiar with surveillance and thus delve deeper into the processes and reduce the overheads in upskilling multiple audit teams.

Chasing Completeness

Achieving completeness of surveillance across trading platforms (including trades, orders, quotes) and communication channels is another common challenge across the industry, fuelled by complex internal processes, systems and data landscapes as well as pragmatic challenges accessing exchange data. Most firms address this challenge in three ways: systematically understanding the gaps; establishing effective new venue processes to avoid an increasing or ongoing problem; and closing identified surveillance gaps. The latter, however, is fraught with challenges relating to data and cost-benefit reservations. Many firms question the cost-effort-benefits of achieving absolute completeness of automated surveillance versus focusing on the more material areas of business activity and mitigating lower risks through periodic monitoring or other means. This is an area where some firms welcome further guidance on achieving the right balance.

Figure 4.1: Completeness grid:



Unknown unknowns: The completeness assessment

Completeness assessments are now becoming commonplace for firms. These assessments look at the extent to which surveillance systems cover all of the trading businesses, systems and data necessary. For large multi-jurisdictional firms, the range of trading teams, exchanges (including RIEs, MTFs and OTFs) and trading systems can be complex and difficult to accurately map. The completeness assessment is an attempt to do so and compare against the range of data feeding into the surveillance tools in order to identify any coverage gaps in trade or communications surveillance coverage.

A challenge with completeness is that inevitably, there may always be unknown unknowns. Whilst from a practical perspective completeness as a concept may never be guaranteed, activities such as a completeness assessment can provide a level of confidence that near completeness exists.

Completeness is a challenge for structured data, mapping exchanges, order management systems and quotes as well as for communications, where the explosion in digital communications channels provides a constant risk for surveillance teams attempting completeness.

Known unknowns: Closing the gaps

Within the spectrum of what is known many firms continue to have trades and, more commonly, orders and quotes that do not feed into the automated trade surveillance. Regulators recognise this but are increasingly unsympathetic "*we now expect firms to be fully compliant with the obligation to undertake quote surveillance*."[3]

There are two drivers that inhibit completeness:

1. External data fairness

   Whilst firms record client orders placed, most firms do not capture orders transmitted to trading platform providers (including RIEs, MTFs and OTFs) meaning that in order to perform surveillance on these orders the data must be provided by the platform provider, of which there may be many used by the firm.

   Platform providers can offer this data on a commercial basis and may choose to do so irrespective of the extent to which the firm uses the platform, be it 5 trades a year or 5000 trades a day. Consequently, in some instances the data cost is considered disproportionate to the risk posed.

   Platform providers are under no obligation to provide the data in any given format and so formats across platforms vary, leading to data integration overheads, and platform providers may vary the format over time, leading to ongoing maintenance issues and overheads.

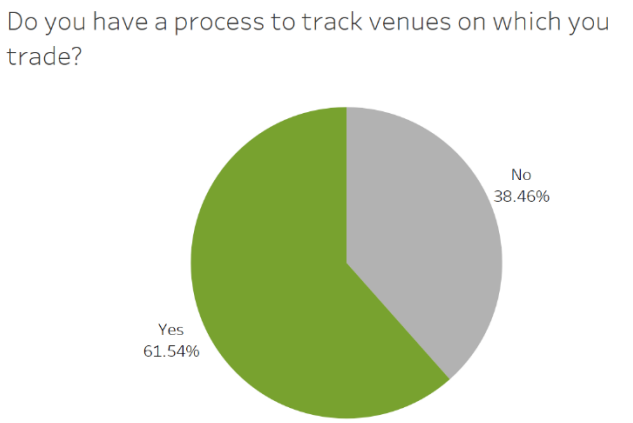
2. Incongruous internal data sources

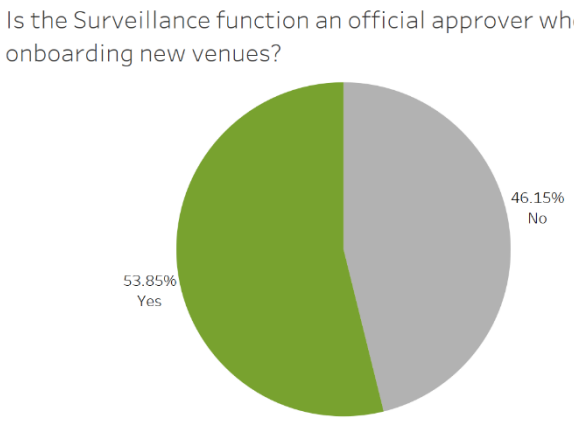
   Internal trades, orders and quotes may be stored in a variety of formats and storage mechanisms. While this is less of an issue for trades, which will generally feed into homogenous formats to feed central settlement and finance systems, for orders and quotes regulation obliges firms to store this data but not necessarily in a consistent format.

   As a result, different order and quote storage systems can require different data ingestion mechanisms and may be available on different timescales.

A simple improvement that some firms have made to improve completeness on an ongoing basis is to make the surveillance team an official approver for onboarding new venues and launching new products. To date just over 50% of firms have implemented this powerful control.

Figure 4.2: Survey responses for venue tracking:





[3] Financial Conduct Authority, Market Watch 58, December 2018

Surveillance team approval at onboarding will create a glide path to completeness but resolving historic gaps will continue to require re-engineering of legacy data frameworks.

Why chase completeness?

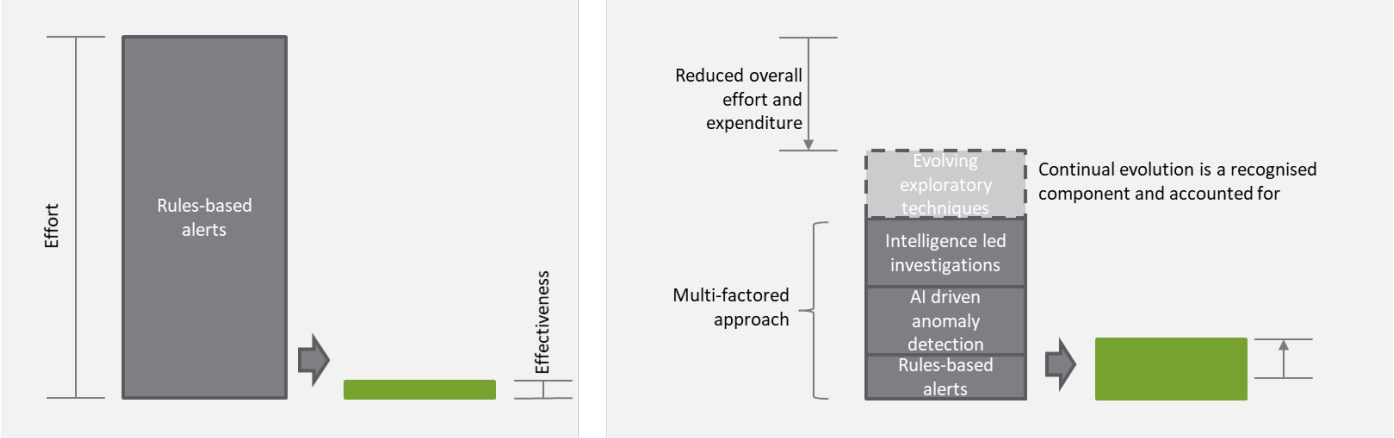
As firms across the industry expend their efforts in mapping data, changing processes, purchasing data, building data lakes and designing data source connectors they find themselves constantly chasing completeness. Some are questioning if the effort adds satisfactory value. Completeness is an easy 'goal' for auditors and examiners: finding a few known gaps in channel coverage or venue coverage is of benefit and addresses non-compliance (at least for trades, orders and quotes). However, arguments exist as to whether completeness should be such an important consideration. Driving surveillance change through what is most easily argued by an auditor or examiner is different to focusing on the most material risks and is perhaps the opposite of 'risk-based'. One interviewee commented "focusing on capturing everything does take away from focusing on genuine risk". There are counter examples: Inter Dealer Broker (IDB) order flow, whilst arguably may be a less likely channel for market abuse, does provide important price discovery. Focusing coverage in a risk-based manner rather than a complete manner will also need its own controls to avoid the conflict of interest of surveillance teams, who may choose to retrospectively identify greater risk in the areas that are already under surveillance. It is true though that the estimated perception of risk will invariably differ from events that occur and there are historic cases of market abuse that remind us that 'LOW risk' does not equate to 'NO risk'. In response, many firms rely on manual surveillance, in addition to automated surveillance to cover risks and data sources not ingested or monitored through automated scenarios.

A change in approach: focusing on effectiveness

With a robust framework established and coverage increased, those firms at the leading edge of surveillance are now looking to tackle the effectiveness challenges inherent within the current model. The audit driven change agenda, whilst clarifying the importance of good practice, has in some instances created self-fulfilling tick boxes as standards. Lexicon based communications surveillance is one such area. Whilst most firms recognise the value of communications surveillance and certain elements of lexicon driven alerts, the focus on expanding lexicons and reviewing every instance of a hit against a broad set of terms is driven more by a desire to avoid the perception of a control gap than on material risk.

In addition to this are areas where good practice is vague and clear audit or assessment points are not easy to articulate or evidence. Investigatory analytics and non-alert driven data-focused reviews are two such areas. It is in these areas that firms report a desire to see advancements, but the vendor innovation is driven by firm requirements which are dictated and prioritised by audit points and assessment comments. For regulators and auditors to take a less tick-box approach and allow scope for innovation requires firms to develop more mature and standardised approaches to measuring, or estimating, control effectiveness. Once firms have measures of effectiveness that they are confident will meet regulatory expectations, then they can proceed in replacing less effective techniques with innovative new approaches. The dawn of a new paradigm for surveillance, away from processing high alert volumes and driven by depth of insight in behaviours, will define surveillance change over the course of the coming years but requires support from industry practitioners, vendors, auditors and regulators alike to achieve.

Figure 5.1: Using increased effectiveness to create efficiency and avoid additive effort:



Communications surveillance

Communications surveillance is not mandated by regulation in Europe, although it is an expectation of many regulators. Given the extremely high false positive rates for communications surveillance, both e-comms and voice, many question the value of communications surveillance and the rationale for undertaking it.

Communications surveillance began as a response to the LIBOR scandal of 2012 and was mandated by US regulator CFTC for certain firms. Through the LIBOR scandal, electronic discovery ('e-discovery') was a key technique used by litigators to uncover wrongdoing and identify evidence. It is on the back of this that firms, advised by their legal teams familiar with e-discovery, began performing regular e-discovery checks that became lexicon-based e-communications surveillance. Communications surveillance expanded to voice and has since become the norm and regulatory expectations have aligned with guidance now referring to this.

Many also question the detective value that communications surveillance provides particularly given its sometimes high cost, due to the vast number of false positive alerts. One interviewee's perspective was that a "lot of overreliance is currently placed on lexicon-based communications surveillance". However, stepping away from what has become standard industry practice presents real or perceived regulatory risk. Firms wishing to do so are focusing on how they can measure surveillance effectiveness to demonstrate more productive alternatives.

Current leading practice in e-communications continues to use lexicon techniques but appends these with metadata-based rules to enable far greater automated removal of clear false positives. Whilst firms that have invested in employing these more advanced approaches do not yet claim greater effectiveness, they have recognised significant efficiency benefits. Firms moving to use these and more advanced techniques such as natural language processing and metadata analysis will also need to keep in mind the additional governance needed over these sophisticated techniques to ensure that risk owners, risk stewards and analysts clearly understand what the techniques employed will and will not identify.

Covid-19 has significantly changed the working environment across the financial services industry and has brought new challenges to the way in which firms consider the extent to which their market abuse control framework is robust and dynamic. The work from home environment that the pandemic has created across the industry has compelled firms to use new communications channels, including video conference. Whilst niche technology solutions exist to monitor video communications most firms currently rely upon audio-only monitoring of video communication channels. Capturing of the audio portion of a video communication is required and tools and techniques to perform surveillance over this are within the existing toolsets of most firms.

Most firms have now adapted their controls in light of the work from home environment by enhancing specific controls where possible. Whilst most surveillance teams understand the need to document this process in their risk assessments, some in the industry feel that there are certain inherent risks for which the controls available will always be limited. The additional risks that employees communicate via unrecorded personal media and the resultant risk of disclosure of insider and sensitive information in a work from home environment are inherent and perhaps cannot be managed in the traditional framework. The big expectations placed upon the bolstering of other controls to mitigate these new and different risks is still an area of debate. We can expect to see further changes to the way that work from home environment is managed particularly as firms consider a hybrid model of office and home-based working.

Investigatory analytics

Much of the current and legacy focus for technology and analytical capabilities within surveillance teams has focused on automated detective functionality, that is the automated generation of alerts. The less well-developed area of analytics within surveillance is investigatory analytics, that is the semi-automated query and visualisation capabilities provided to surveillance analysts to support their triage, review and investigation of alerts. Many trade surveillance vendor tools, and some communications tools, provide some element of investigatory analytical capabilities. However, like detective scenarios, investigatory analytics approaches cannot be simply 'out-of-the-box' generic approaches but rather need to be configured to specific products, markets and booking models if they are to be effective.

Regulatory guidance, investigatory guidance and industry standard on good practice are less well-developed in investigatory analytics than detective analytics. This has led to check and challenge teams, including internal and external audits to focus less on this. The depth of investigation is also inherently difficult to assess. With less prescriptive standards available it can be difficult for firms to identify a clear need to develop further in this area. However, many experienced surveillance leaders identified this as an area where further development is needed. A desire for greater contextual analysis providing investigators with a risk view of a trader or clients entire aggregated activity across products, across books and across time enables more insightful assessment of even the most innocuous of 1st level alerts but requires considered design and not insignificant data plumbing. An example provided by an interviewee was of a firm using social network analytics across publicly available data to identify a link between a client and an issuer that helped bolster an insider dealing STOR beyond the transaction activity only - demonstrating the value of advanced tooling and inquisitive analysis. Greater articulation of the importance of investigatory analytics and the definition of good practice is needed to support its development. Only with a shared definition of good practice will this drive a focus from auditors and examiners, which in turn will drive and support a greater focus from firms, which will sponsor greater innovation from vendors in this area.

A new paradigm

Some firms are beginning to take investigatory data analytics a step further and are asking their teams to undertake deep data-driven investigations but not in response to any alert but rather in response to a perceived and specific area of risk. For example. a particular market event or market shock, or a high risk set of customers over a specified period. Some are hope that developments in using cluster analysis and trader, client or desk risk scoring can allow reviews to focus on entity level risk rather than transaction level alerts and ultimately move away from the high-volume alert filtering currently absorbs the time and focus of investigators. A similar concept has been deployed in AML transaction monitoring teams, where it is sometimes referred to as "intelligence-led" investigations, and received acclaim from those absorbing the output. Proponents of this change in approach for surveillance recognise the challenges ahead to make this a well-accepted surveillance technique, not least that the regulation specifically references automated alerts. But if firms can develop robust techniques to measure effectiveness then demonstrating the evidence to move from legacy techniques to more innovative approaches will become possible – without putting one's head above the perceived regulatory parapet of status quo.

Conclusion: Where next?

This paper has summarised information gathered from a diverse subset of AFME members, to lay out the current state and drivers for change in surveillance activity and subsequent governance principles. Five key areas of focus have been discussed, but what are the pragmatic next steps for financial institutions as they seek to enhance and maintain effective governance over surveillance controls?

What is clear, based on information gathered and our experience in the market, is that firms of different sizes with different branch structures in different jurisdictions will not always face the same challenges in maintaining 'good governance'. There is no 'one size fits all' solution, however there is value in weighing up the potential benefits of factoring in the following five areas as part of a future looking governance framework:

Aligning surveillance talent to markets rather than systems	The benefits and efficiencies of moving away from bifurcated surveillance teams across trade and communications, in favour of integrated teams that have product and market specific skill sets are clear. Moving towards this type of organisational model is a step towards developing a more holistic investigation capability, where analysts are empowered to build and understand the full picture around any given alert, albeit for now across disparate alerting systems. This model does not come without its own challenges, especially for institutions of bigger scale, but firms should assess whether there is enough benefit to pursue this rather than rely on legacy structures that may not be fit for purpose.
Have clearly delineated processes that balance oversight vs independence	Maintaining robust oversight over the surveillance function is crucial in ensuring effective surveillance is carried out, however firms should continue to consider any potential conflicts of interest, especially where investigating and reporting internal activity. Well documented, well thought through and well followed processes mean that navigating conflicting risks is not reliant upon the nous of individuals
Review the framework of components that support and maintain core surveillance processes	Without a coordinated and well-defined framework to support, maintain and govern core detective processes, surveillance cannot remain sustainably compliant and risk based. Processes such as MI, risk assessments, tuning and calibration, QA, governance committees and independent reviews all need to be part of this and work in concert to drive an efficient and agile control structure. Get the framework right now before embarking on a journey of improvement to support controlled change.
Work with regulatory bodies to workshop the potential of moving towards more risk driven and intelligence led surveillance	Once firms have measures of effectiveness that they are confident will meet regulatory muster, then they can proceed in replacing less effective techniques with innovative new approaches. The dawn of a new paradigm for surveillance, away from processing high alert volumes and driven by depth of insight in behaviours, will define surveillance change over the course of the coming years. In order to succeed, this will require support from industry practitioners, vendors, auditors and regulators alike.
Balance the focus on detective vs investigatory capabilities	As firms move towards more risk driven methods of surveillance, the importance of advancing investigatory capabilities will become more prevalent. More advanced functionality will give analysts the tooling needed to conduct in depth and meaningful investigations, and vendors have a part to play in understanding the new requirements and providing solutions that give investigators the ability to scrutinise complex data.

AFME members have demonstrated that they are already considering the areas outlined above, however there are factors outside of firms' control that may inhibit or accelerate improvements across the industry.

Regulatory bodies should empower firms to innovate and find more effective ways to conduct surveillance with the aim to ensure markets are fair and transparent. Open dialogue and a willingness to engage between firms and regulatory bodies continues to be crucial as is agreeing a consistent approach to estimating, measuring and communicating effectiveness. Innovation requires regulators, practitioners, auditors and vendors to work collectively, with the same aim in mind, and with greater collaboration to help drive consistency in surveillance standards and governance as we move into the next era of surveillance. As firms come towards the end of the era of increasing coverage, they should look now focus on the era of increasing effectiveness whilst remaining cognisant of the challenges that lie ahead.

Appendix

Table 1: Applicable regulatory and industry guidance

#	Regulatory Body	Document Title	Website Link	Page Reference
1	European Union	Market Abuse Regulation	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0596&from=EN	Pg. 9 (46)
2	European Union	COMMISSION DELEGATED REGULATION (EU) 2016/957	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0957	All
3	Futures Industry Association	Surveillance and Market Practices: Guidelines for market participants in respect of Market Abuse Surveillance requirements prescribed under the Market Abuse Regulation (MAR) when trading derivatives	https://www.fia.org/sites/default/files/2020-09/FIA_WP_Market_Surviellance%20%281%29.pdf	All
4	Financial Conduct Authority	Guidance on financial crime systems and controls: insider dealing and market manipulation	https://www.fca.org.uk/publication/finalised-guidance/fg18-05.pdf	Pg. 86-88
5	Financial Conduct Authority	Market Abuse in a time of coronavirus	https://www.fca.org.uk/news/speeches/market-abuse-coronavirus	All
6	Financial Conduct Authority	Market abuse requires a dynamic response to a changing risk profile	https://www.fca.org.uk/news/speeches/market-abuse-requires-dynamic-response-changing-risk-profile	All
7	Financial Conduct Authority	SUP 15.10 Reporting suspicious transactions or orders (market abuse)	https://www.handbook.fca.org.uk/handbook/SUP/15/10.html	All
8	FICC Markets Standards Board	Surveillance Core Principles for FICC Market Participants: Statement of Good Practice for Surveillance in Foreign Exchange Markets	http://www.femr-mpp.co.uk/wp-content/uploads/2016/12/16-12-08-SoGP_Surveillance-in-FX-Markets_FINAL.pdf	Pg. 11, Core Principle 3
9	FICC Markets Standards Board	Monitoring of written electronic communications	https://fmsb.com/wp-content/uploads/2017/09/FMSB-SGP-Monitoring-of-written-E-comms-Final.pdf	All
10	FICC Markets Standards Board	Suspicious Transaction and Order Reporting	https://fmsb.com/wp-content/uploads/2019/01/Suspicious-Transaction-and-Order-Reporting-Statement-of-Good-Practice-for-FICC-Market-Participants.pdf	All
11	FICC Markets Standards Board	Statement of Good Practice for FICC Market Participants: Conduct Training	http://www.femr-mpp.co.uk/wp-content/uploads/2016/12/16-12-08-SoGP-Conduct-Training_FINAL.pdf	Pg. 5 – reference to Market Abuse training
12	Global Foreign Exchange Committee	FX Global Code	https://www.globalfxc.org/docs/fx_global.pdf	All

13	Bank of England	The UK Money Markets Code	https://www.bankofengland.co.uk/-/media/boe/files/markets/money-markets-committee/uk-money-markets-code.pdf?la=en&hash=C7854B22B681B65244EE35A8CC306288454B4506	All
14	LBMA	Global Precious Metals Code	http://www.lbma.org.uk/downloads/PMC2018.pdf	All

Acknowledgements and Contacts

We are grateful to AFME Surveillance Working Group members who contributed their time and thoughts in producing this report. The Working Group comprises EMEA heads of surveillance from AFME members. Our European Compliance work programme focuses on influencing the European regulatory environment to foster a culture of integrity and effective conduct regulation.

The data in this report comes from interviews with 8 of those Members, and survey responses from 18 members, representing a variety of geographical locations and business models.

www.afme.eu/Divisions-and-committees/Compliance

We are also grateful for the input of 2 European regulators who agreed to be interviewed for this report.

AFME Contacts

Richard Middleton
Managing Director,
AFME
richard.middleton@afme.eu
+44 (0) 203 828 2709

Louise Rodger
Director, Compliance
AFME
louise.rodger@afme.eu
+44 (0) 203 828 2742

Giovambattista Perrotta
Policy Associate,
AFME
giovambattista.perrotta@afme.eu
+44 (0) 203 828 2699

EY Contacts

Stuart Crotaz
Partner,
Conduct and Compliance
EY LLP
scrotaz@uk.ey.com
+44 (0)20 7951 9714

Tom Goodman
Senior Manager,
Financial Crime and Forensics
EY LLP
tgoodman1@uk.ey.com
+44 (0)20 7806 9675

Luke Russell
Senior Associate,
Conduct and Compliance
EY LLP
lrussell2@uk.ey.com
+44 (0)20 7783 0112

London Office
39th Floor
25 Canada Square
London E14 5LQ
United Kingdom

Switchboard:
+44 (0)20 3828 2700

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium

Switchboard:
+32 (0)2 788 3971

Frankfurt Office
Bürohaus an der Alten Oper
Neue Mainzer Straße 75
60311 Frankfurt am Main
Germany

Switchboard:
+49 (0)69 153 258 967

AFME is registered on the EU Transparency Register, registration number 65110063986-76