

Enhancing data quality for effective Surveillance in Capital Markets

September 2024



Disclaimer

AFME's *Enhancing Data Quality for Effective Surveillance in Capital Markets* (the "Paper") 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 does not represent or warrant that the Paper 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/aboutus/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).

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

September 2024

Contacts

AFME



Louise Rodger
Managing Director
Louise.Rodger@afme.eu



Shalini Cautick
Associate
Shalini.Cautick@afme.eu

KPMG



Lucas Ocelewicz
Partner
Lucas.Ocelewicz@KPMG.co.uk



Aaron Stowell
Partner
Aaron.Stowell@KPMG.co.uk



Dharam Shah
Director
Dharam.Shah@KPMG.co.uk



Louis Cottell
Senior Manager
Louis.Cottell@KPMG.co.uk

Contents

Foreword	2
Executive Summary	3
1. Background and introduction	4
2. Key themes and recommendations	7
3. Data management and governance	12
4. Opportunities for improvements in data quality	17
5. Data ownership	20
6. Surveillance data in practice	23
Summary of recommendations	24
Conclusions and next steps	26
Appendix A: Third-party data provider questionnaire	27
Appendix B: Surveyed challenges	28



Foreword

AFME is pleased to publish “Enhancing data quality for effective Surveillance in Capital Markets” in collaboration with KPMG. This report comes at a critical time, with surveillance increasingly in the regulatory spotlight.

The introduction of the European Market Abuse Regulation (MAR) set new obligations for surveillance. Several years on from that and in light of recent high-profile enforcement cases, there is growing regulatory pressure for firms to assess both the coverage and quality of the data that forms part of their surveillance efforts to detect and investigate market abuse.

Our 2019 AFME/KPMG report “The Future of Surveillance in Wholesale Banking”¹ focused on the evolution and future strategies of the surveillance function: this paper focuses attention on the importance of data quality ensuring firms’ foundations are fit for purpose.

What becomes very clear is that without complete, accurate and timely data, firms are unable to run effective surveillance controls and nor are they able to fully leverage advances in technology, all of which impacts their ability to detect various forms of market abuse.

This paper outlines key considerations for how firms can improve their data quality, data ownership and data governance standards, as well as highlighting the critical data elements required to detect behaviors and as a result develop robust data governance frameworks.

This paper provides a set of best practice approaches for managing surveillance data to help drive better quality standards across the industry and increase the effectiveness of surveillance processes.

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



James Kemp
Managing Director
GFMA & AFME

¹ AFME/KPMG “The Future of Surveillance in Wholesale Banking” October 2019



Executive Summary

Surveillance has increasingly been in the regulatory spotlight as a result of high-profile enforcement actions. Firms face a multitude of challenges relating to the differing data standards across trade and communications surveillance, which creates inconsistencies across the industry of ensuring effective surveillance. Firms also experience difficulties in collecting complete and timely data across trade and communications surveillance. Without complete, accurate and timely data, firms are unable to run an effective surveillance control, which limits their ability to detect forms of market abuse.

The findings in this paper are based on industry feedback and whilst there is significant discussion on artificial intelligence and bold visions of future surveillance, today firms need to focus on getting the core requirements right. Without good quality data, firms will not effectively leverage advances in technology and analytics and risk compromising their ability to prevent and detect market abuse risks. There is a key dependency on quality data for effective surveillance. For example, the quality of alert output by surveillance models is heavily dependent on factors such as completeness, accuracy, and timeliness of data.

We encourage firms to consider how they might adapt and evolve their approaches to data based on four core areas; 1: data management and governance, 2: opportunities for improvements in data quality, 3: data ownership and 4: surveillance data in practice and provide a series of recommendations on page 24.

“Firms face a multitude of challenges relating to the differing data standards across trade and communications surveillance, which creates inconsistencies across the industry of ensuring effective surveillance”



1. Background and introduction

1. Background and introduction

“Firms cannot confidently comply with MAR unless they have strong data governance”

Overview of surveillance within the industry

In July 2016, the European Market Abuse Regulation (‘MAR’) came into force, carrying criminal sanctions for a range of prohibited behaviours for firms and individuals. The regulation aims to protect the integrity of financial markets by prohibiting abusive practices that (i) artificially manipulate or distort prices or (ii) promote the misuse of confidential information for illegitimate purposes. The regulation prohibits any actions designed to artificially manipulate the price of or market for a financial instrument, including the spread of false rumours or engagement in misleading trading practices. To achieve these objectives, MAR imposes strict obligations on firms when they are issuing financial instruments or engaging in certain practices that could be manipulative, such as spreading false or misleading information, creating misleading buy or sell orders, and engaging in other deceptive trading practices. To comply with MAR, firms must implement robust systems for detecting and preventing market abuse, while national authorities are empowered to investigate suspicious activities and impose sanctions for any breaches of the regulation. By promoting transparency, fairness, and investor protection, MAR plays a vital role in fostering trust and confidence in financial markets, creating a more stable and reliable environment for all participants. Since the allegations of widespread market abuse emerged over a decade ago relating to the manipulation of LIBOR and global foreign exchange markets, there has been a clear focus on firms to address and remediate such issues by global regulators. The LIBOR and FX cases resulted in upwards of \$19 billion in fines.

In addition to this, high profile misconduct cases have resulted in significant regulatory focus on surveillance² with firms applying rigorous techniques to identify, detect and investigate market abuse. This often takes the form of rule-based detection models to identify problematic behaviour patterns or the development of more sophisticated and complex models.

More recently, we have seen regulatory and market focus shift towards the quality of data feeding these models, with greater expectations on firms to develop and maintain a robust data management framework, which advances the efficacy and effectiveness of surveillance functions. Alongside this, firms must comply with MiFID II record-keeping requirements, which for firms means retaining records relating to trade, pre-trade, communications, and client data. Failure to maintain complete, accurate and timely (‘CAT’) records has front to back implications across a number of functions including the ability for firms to undertake effective surveillance.

Regulatory expectations for CAT data is further reinforced by a number of higher profile fines for firms where issues relating to inadequate data quality³ have impacted the effectiveness of surveillance controls.

As illustrated below, failures in surveillance data quality have resulted in several recent enforcement cases and regulatory fines. Since 2021, \$1 billion has been issued in fines by regulators relating to data failures.

² For the purposes of this paper, surveillance has been defined as detecting and investigating activity for signs of market abuse, through trade and communications detective controls.

³ For the purposes of this paper, data quality refers to completeness, accuracy, and timeliness



Regulatory data-based sanctions



Case 1

In 2021, a major firm faced significant penalties totalling \$200 million from US regulators for widespread and long-standing failures in maintaining and preserving communications data. Equivalent enforcement actions were also levied against a number of other similar firms and this topic remains an industry wide concern, as demonstrated in Case 2 below. The firm's employees routinely used personal devices and third-party messaging platforms, including personal email accounts, SMS text messages, and WhatsApp, to discuss business matters without properly retaining or preserving these communications. The lack of comprehensive recordkeeping hindered regulatory investigations and resulted in the firm's inability to produce complete records when requested. Regulators emphasized that this case represented the largest-ever financial sanction related to recordkeeping failures.

In 2024, the same institution faced fines totalling \$448.2 million and regulatory scrutiny when it discovered significant gaps in its trade surveillance program. These gaps stemmed from the firm's failure to properly configure surveillance data feeds from multiple trading venues and systems, resulting in incomplete trade and order data being ingested into its surveillance tools.

As a result, the firm failed to surveil billions of order messages over several years on a particular US exchange, primarily related to electronic trading activity. This oversight was attributed to an erroneous assumption that data directly from exchanges was inherently reliable and did not require verification. The firm has since taken steps to remediate these surveillance gaps.

This highlights the critical importance of:

- Data integrity and completeness: data repositories must ensure the integrity, completeness, and accuracy of captured communications data. The case serves as a stark reminder for firms to prioritize robust recordkeeping practices concerning data and the serious consequences for non-compliance.
- Comprehensive data ingestion: ensuring that surveillance systems receive complete and accurate data from all relevant trading venues and systems.
- Data validation and reconciliation: implementing robust processes to validate data accuracy and identify discrepancies, regardless of the source.
- Regular system testing: conducting thorough and regular testing of surveillance systems to identify and address potential gaps or vulnerabilities.



Case 2

In 2023, a regulatory agency levelled charges against multiple financial firms for significant and ongoing failures to maintain and preserve electronic communications data. Firms, which included broker-dealers and investment advisers, admitted to violating recordkeeping provisions of federal securities laws. These violations involved employees at various levels of authority, including supervisors and senior executives.

The firms acknowledged that their employees frequently used personal devices and third-party messaging platforms for business-related communications, which were not adequately maintained or preserved. The lack of recordkeeping relating to data hindered the regulatory agency's ability to oversee compliance and conduct investigations effectively.

As a result of these violations, the firms agreed to pay substantial combined penalties totalling \$289 million. They also agreed to cease and desist from future violations, implement improved compliance policies and procedures, and retain independent compliance consultants to review their practices.

This case highlights the critical importance of:

- Recordkeeping for investor protection and market integrity: these actions serve as a reminder to all regulated entities to prioritize compliance with recordkeeping requirements and to self-report any violations promptly.



1. Background and introduction

Why is this paper important?

As evidenced in the cases above, there has been growing regulatory pressure on firms to assess the coverage and quality of the data that forms part of the Surveillance function. This has materialised in a series of data-related fines, directed at some of the market's leading firms from a range of global regulators.

The paper aims to explore the following areas:

Section 3: Data management and governance

Section 4: Opportunities for improvements in data quality

Section 5: Data ownership; and

Section 6: Surveillance data in practice.

The information in this paper is based on the opinions of well-informed and experienced industry market participants from over eighteen firms and KPMG's specialists, obtained via a survey and a series of structured interviews with a subset of AFME members. The overarching themes have been summarised in the following section, with subsequent sections illustrating key discussion points based on survey and interview results with AFME members, across each of the four areas listed above.

To ensure appropriate representation, participating firms comprised various size and scale with geographical spread of head office locations, including France, Germany, Switzerland, Spain, the UK and the USA. A complete list of members can be found at www.afme.eu. The figures in this paper are based on the results of questions answered by interview participants.

“There has been growing regulatory pressure on firms to assess the coverage and quality of the data that forms part of the Surveillance function”



2. Key themes and recommendations

The following key themes and recommendations are areas that firms and surveillance functions could address in order to reduce the risk of failing to prevent or detect market abuse as a result of poor-quality data. We have identified five key themes from the four sections outlined below: *data management and governance, opportunities for improvements in data quality, data ownership; and surveillance data in practice.*

2.1 Poor quality data increases market abuse residual risks

Whilst most surveillance functions assess the inherent and residual risks of specific market abuse behaviours across different products / business lines, explicit consideration of the quality of data inputs used by surveillance does not currently form part of most control effectiveness assessments, which risks leading to an overstatement of control effectiveness. Historically, firms managing competing priorities have tended not to prioritise consideration of data quality as a standalone issue nor conversely, the implications of poor data quality in their market abuse risk assessments.

What practical steps could firms take to address data quality issues and uplift their market abuse risk assessments?

Firms should now consider incorporating data feed completeness, accuracy and timeliness when reviewing the effectiveness of their controls and when assessing the residual risk for market abuse behaviours across products / business lines. This would directly benefit the assessment of control coverage, leading to more informed residual risk ratings and therefore driving more effective and strategic surveillance solutions. Failing to do so will lead to:

- Understated residual risk: without confidence in data quality, residual risks may be skewed, leading to an inaccurate view of risk exposure.
- Ineffective surveillance: incomplete or inaccurate data undermines the effectiveness of surveillance, increasing the risk of undetected market abuse behaviours.



Without firms becoming aware and considering the questions above when completing their market abuse risk assessments, there is a risk that MAR offences may go undetected at firms resulting in further enforcement activity, regulatory fines, and reputational harm.



2. Key themes and recommendations

2.2 Knowing where your data is coming from and how it is being used

A second important area of focus for firms is having a clear understanding of the data flows that are used for market abuse prevention and detection and the integrity of their sources. Failure to gain this understanding could result in difficulties when applying ongoing governance over data. It is important to note that this paper is not advocating for surveillance functions to be solely responsible for reconciling and mapping all relevant surveillance data feeds. Instead, this paper outlines the importance of surveillance collaborating with 1st Line (Business and Technology) in documenting appropriate data sourcing which will allow surveillance functions to have a clear understanding of data sources relevant to surveillance. This exercise will have to be performed in line with the priorities and budgetary constraints of individual firms.

Why is data sourcing important?

Without a clear line of sight for all relevant data sources, it is difficult to assess the completeness of data coverage and whether there are adequate CAT controls in place that ensure the quality of data feeding into downstream surveillance systems.

This is also applicable to data sourced from third party venues. Given recent regulatory enforcement actions relating to venue data and completeness, firms should ensure they have a reconciliation process to compare the CAT of data from venues to their internal records.

Without knowing where the firm is getting data from with a clear line of sight, it is difficult to identify and assess the impact of upstream changes, for example, whether repository changes to timestamps may compromise downstream surveillance alerts effectiveness.

Fundamentally, without a clear front to back view of end-to-end data inputs, it is extremely difficult to identify crucial gaps. Firms do not know what they are missing and there is little visibility on whether data is complete, accurate and timely. It should be noted that firms should do this in conjunction with improving transmission methods to take steps to ensure that data completeness is maintained.

What practical steps could firms take to document their end-to-end data sources?

As mentioned above, surveillance functions could partner with business and/or IT functions to strengthen internal governance and to understand the sources of surveillance data flows, including any modifications or enhancements that are made to the data upstream.

As a best practice, this could be documented as part of a data flow mapping which is regularly reviewed and assessed. The scope of data from external sources should also undergo periodic attestation from accountable business representatives, including which venues and/or platforms the firm uses for pre-trade and trade execution activity.



2.3 Lack of clarity in internal data ownership

It was highlighted through in-depth interviews that surveillance functions are sometimes responsible for the CAT of data “one hop” up from the data flow, for example from an intermediary data repository to the trade surveillance system. Through these interviews, it was identified that there is often a lack of clarity of who is responsible for the CAT of data from internal upstream sources, which can be multiple “hops” from when the data is utilised in the surveillance system.

We note that it is best practice for the 1st Line / producer (the business) to own documenting appropriate data sourcing, as well as any required remediation, if gaps are identified. If data producers enhance data transmission methods and better manage the CAT of data, then this more proactively addresses the root cause of any potential issue. Surveillance is typically the consumer of data, however, where a surveillance function enriches data, if that data is provided to other parties, then surveillance becomes the data producer and should be responsible for documenting appropriate data sourcing and the remediation of any identified gaps.

It was also indicated through the interviews conducted with AFME members that there can be a lack of clarity regarding who is responsible for the quality of data in central data repositories, which typically hold data sets that are used for firm-wide purposes outside of surveillance (for example, for market risk, finance and transaction reporting purposes). This lack of clarity could lead to issues with data quality, due to data not being properly recorded and/or maintained.

What practical steps could firms take to clarify ownership and therefore trust in their data?

When assessing and assigning ownership firms should consider:

- Identifying ownership when documenting end-to-end data sourcing, as well as assessing and identifying which stakeholders need to be held accountable for the completeness, accuracy, and timeliness of key surveillance data sources and feeds.
- An assessment of how involved surveillance should be in a firm’s data governance framework.
- When a function enriches data, who is responsible for the data’s completeness, accuracy and timeliness?
- Once confirmed, roles of data owners and data recipients should be documented, and periodically reviewed and updated if needed, as part of a data service level agreement.
- Who owns surveillance data from a Senior Manager Regime (SMR) perspective and what upstream and downstream dependencies are required for them to undertake their role?

However, a one size approach to ownership is not practical and firms will need to implement their own bespoke approaches to ownership and roles and responsibilities based on their own internal structures.



2. Key themes and recommendations

2.4 Preventative and detective surveillance controls rely on a variety of data sources, viewed holistically, to drive insights

Many surveillance scenarios rely on data from more than one source to detect potential market abuse and there is a dependency on the completeness, accuracy, and timeliness of data in order to drive better outcomes in market abuse risk detection.

However, there are challenges with this model, partly due to differences and fragmentation in structured and unstructured data. Data formats, schemas, and structure vary widely across data providers and consumers, with firms using a wide variety of providers. This complexity creates obstacles in implementing impactful surveillance, for firms as data consumers, as they need to cleanse and standardise data from numerous sources to ensure the quality of the data is maintained when ingested into the surveillance systems. This of course becomes more difficult with non-standardised data.

Additionally, advanced analytics, including machine learning and artificial intelligence, are not effective without foundational elements of data quality. Lack of high-quality data will limit the ability to deploy market leading technologies in the future. Firms leveraging repositories with standardised surveillance data, in order to undertake advanced analytics, are likely to achieve better results both now and in the future. It is noted that for many firms this is more of an aspirational target, and in the near term it may prove to be more realistic (and similarly effective) to perform analytics on trade and communications data in separate repositories.

Unstructured and structured data

This risk is particularly relevant in relation to mobile communications, for example in relation to voice, SMS and chat, as these communications methods originate from a variety of global service providers. Many chat-based communication platforms are new to the market and constantly evolving adding new features and capabilities. As a result, it can be extremely challenging to capture the necessary data in the required format

A significant trade surveillance challenge is that data is often siloed within individual platforms or venues, leading to fragmentation, and complicating the ability to gain a holistic view of market activity. This fragmentation can affect the detection of cross-market/product manipulation strategies, as well as creating complexities through the high volumes of data feeds from numerous sources being time intensive to manage and multiplying the challenges in detecting issues with individual data feeds when the feeds are so numerous.

The absence of standardised data formats, schemas and transfer protocols heighten data complexity and fragmentation. For example, inconsistency in timestamps, identifiers, order data and message fields make data aggregation and analysis onerous and risks delaying the detection of potential market abuse.

We recognise that this issue is not just caused by third-party providers and that sometimes firms will have unsuitable internal data sources and standards, for example pre-trade and trade execution data being stored in disparate formats on a range of platforms / mechanisms. Pre-trade data (namely orders, indications of interest and quotes) is a key component in the detection of some market abuse behaviours, therefore capturing and recording consistently formatted pre-trade data in a timely manner remains an issue where firms could benefit from remediation.



What practical steps could firms take to combat complex, fragmented and non-standardised data to implement and maintain detective surveillance controls with better outcomes?

- It may not be efficient, necessary, or effective for some firms to combine all data into one standardised format in a single repository to detect market abuse risks. Incremental improvement may yield sufficient results. It is important not to get side tracked by seeking completeness for completeness's sake, by aggregating all data into one standardised store, as this is not a guarantee of a targeted or efficient solution. Surveillance models ingest specific critical data elements to detect market abuse behaviour. Firms could map market abuse scenarios to the relevant data points at each stage of the scenario to identify and retrieve the necessary data on a priority basis.
- Good quality surveillance controls rely on various data sources. Firms could identify these sources mapped to market abuse risks and focus on refining, reformatting, and transforming key data used for surveillance.
- Most firms have not sought to combine communications and trade data, which does not move the dial on all risks but may potentially facilitate better detection for risks such as front running. This should be a consideration once firms have got their data controls right for both communications and trade surveillance.

2.5 Inconsistent governance standards amongst third parties

Some third parties may still be in the process of establishing data governance and controls over the completeness, accuracy, and timeliness of data that meet evolving industry standards and expectations. Financial services firms have been subject to regulatory enforcement and remediation programmes, which has improved the robustness of their data governance frameworks. The lack of common data governance structures amongst third parties creates uncertainty within surveillance functions for data reliability, thus impacting the confidence in surveillance performed. The view amongst the majority of firms interviewed is that third parties should adhere to more common, robust data governance standards. This would provide the data consumer with greater confidence and assurance in the integrity of the data they receive.

What practical steps could firms take to become more confident in data from third parties?

Where applicable, firms could assess third-party data providers against the Digital Operational Resilience Act ('DORA') principles and standards, evaluating their overall compliance with DORA, data governance, data quality monitoring and data lineage tracking. We have created a template of questions within Appendix A that can be considered when gathering information from third-party data providers. By implementing enhanced due diligence, firms can gain more confidence in the integrity of third-party data.

We note that third-party data providers would be subject to DORA via regulated institutions, whereby firms would deem third-party data provider services to be material or critical.



3. Data management and governance

3. Data management and governance

3.1 Data governance standards

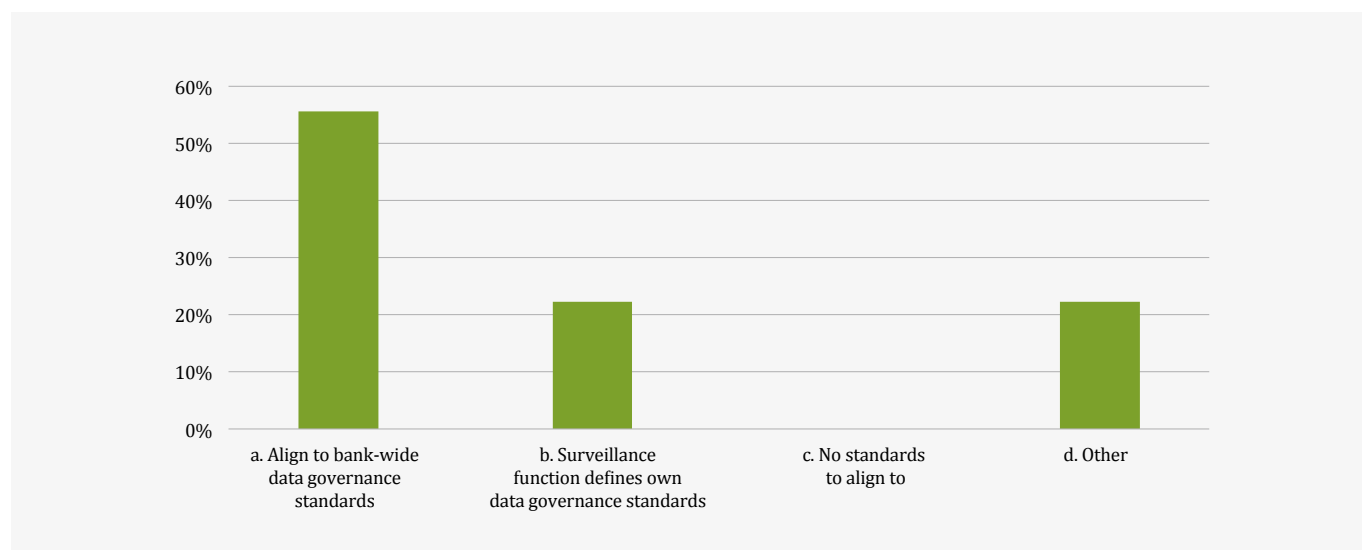
What are the current challenges and implications of an absence of common industry standards to the current state of data governance at firms?

The absence of industry wide data governance standards over time has led firms to prioritise different data governance factors, such as data transfer, storage, privacy and quality. This paper intends to create a point of guidance to drive common industry standards which will lead to a degree of certainty in expectations compared to what firms have, or realistically can, achieve in this area.

The absence of industry wide data governance standards within surveillance means that most firms tend to rely on broader firm-wide data governance standards that may not be directly applicable to surveillance data (See Figure 1). In some cases, surveillance has overlaid, on top of firm-wide standards, surveillance specific data governance standards or implemented a hybrid model across the two approaches (both firm wide standards and more specific surveillance data standards). Where firms employ a common data layer, i.e., data can be sourced once and used many times across different functions, it is expected that surveillance would align to firm-wide standards.

Some firms have a more fragmented approach, with surveillance implementing standards within silos, but are working towards common firm-wide standards in the future.

Figure 1: **How does Surveillance ensure effective data management is in place?**



Where firms responded 'Other', it was often the case they followed firm-wide data governance standards but also implemented surveillance standards for specific processes which were not formalised.

How can firms start to address this issue?

Firms should focus on increased collaboration and discussion of the current state of market and industry practices relating to data and enhancing data quality. Increased collaboration will also highlight common challenges and may promote innovative and holistic solutions.



3.2 Non-standardised data and inefficiencies in the current state

What are the current challenges and implications of non-standardised data?

We note that firms across the industry utilise different data capture and storage solutions, resulting in inconsistencies in data formatting and ingestion into surveillance systems.

Without standardised data formats and schemas, performing effective surveillance becomes more challenging, as it can affect the quality of alert output and impair an analyst's ability to interpret data effectively. To achieve higher quality alerts, data needs to be manipulated or standardised prior to ingestion into surveillance systems or through embedding an extraction transform load ('ETL') process. Firms have a choice between poorer quality alerts with more time spent reviewing by analysts, or increased costs due to investing in ETL processes or expensive third-party systems that can effectively review different data formats and schemas.

The fragmentation of data sources used by firms adds further complexity to data quality. Firms often collect data from multiple internal and external sources, such as trading venues, brokers and communication channels. The integration of these fragmented data sources, where applicable, poses challenges in ensuring data completeness, accuracy, and timeliness.

3.3 Are data lakes / common data layers / repositories the solution?

What is the current state and current challenges?

Most interviewed firms use a hybrid model for structured data, with some data being sourced from a central repository or data lake, and some being sourced from various upstream systems. Many firms have now partially implemented, or are working towards, a common data layer for surveillance purposes.

For communications surveillance, most firms have, or are working towards, a 'golden source' for monitored individuals, which includes who is in scope for monitoring, why they are in scope, their relevant activities, what systems they should have access to and their IDs / aliases.

An equivalent common data layer for both communications and trade data is significantly more challenging to realise because of specific sets of requirements for both communications and trade. Issues such as data privacy and a lack of common structured data attributes across communications, order and trade, limits the overall benefit of establishing a common data layer across these record types. Another challenge relates to managing what will be considerably large volumes of data. For example, to leverage the benefits of artificial intelligence and its anticipated future widespread use, firms will need to merge both data sets resulting in significantly large data volumes, which will likely be difficult to store and process in a single layer.

Structured and unstructured data sets also require different database technologies in order to have efficiency in data storage and retrieval, adding another layer of complexity to a common data layer.



3. Data management and governance

How can firms address current state challenges?

As data consumers, surveillance functions often do not have control over the CAT of data arriving from upstream sources. However, there is a growing regulatory expectation for data consumers within firms to be confident in the reliability of the data they receive. One suggested approach made by some firms we interviewed is to establish a business owned central data repository that is recognised and maintained as an authorised data source. This would mitigate some of the risks associated with the various steps in the data journey from an upstream source into a surveillance tool.

Irrespective of whether data is being sourced from a central data lake or distributed repositories, surveillance teams must be highly confident in the CAT of the data they use. This could be supported by clear data sourcing documentation, and proactive engagement with data providers and the front office to ensure the data integrity of information feeding into surveillance processes. Without this assurance, even the most sophisticated surveillance tools will struggle to effectively detect market abuse.

Figure 2: **High level diagram of data flow without common data repository**

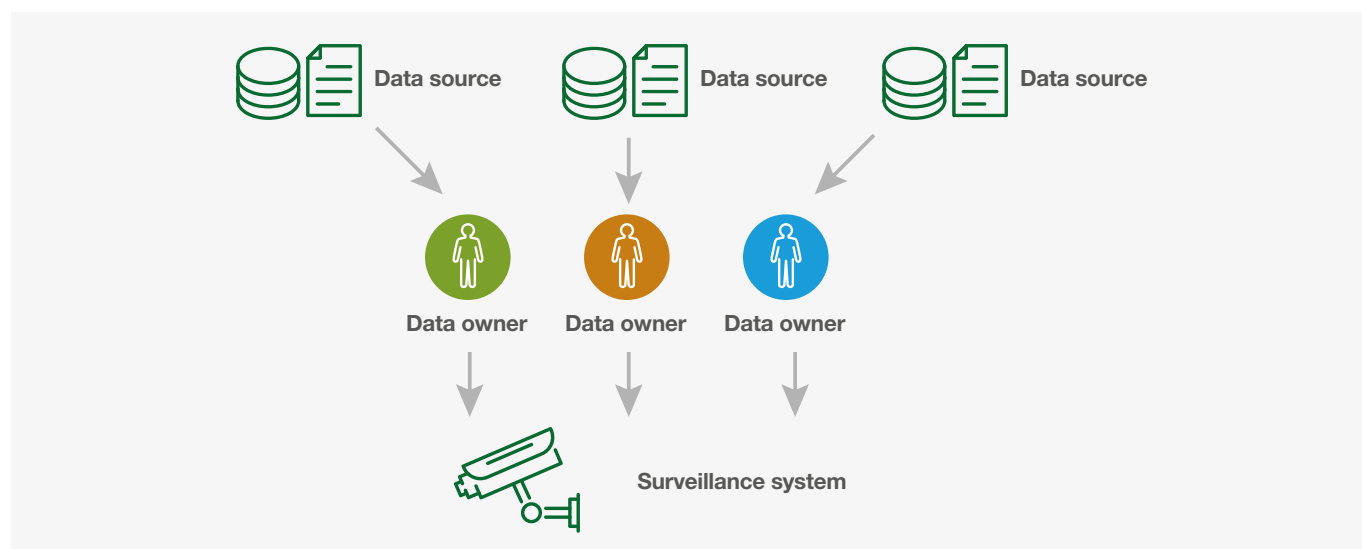
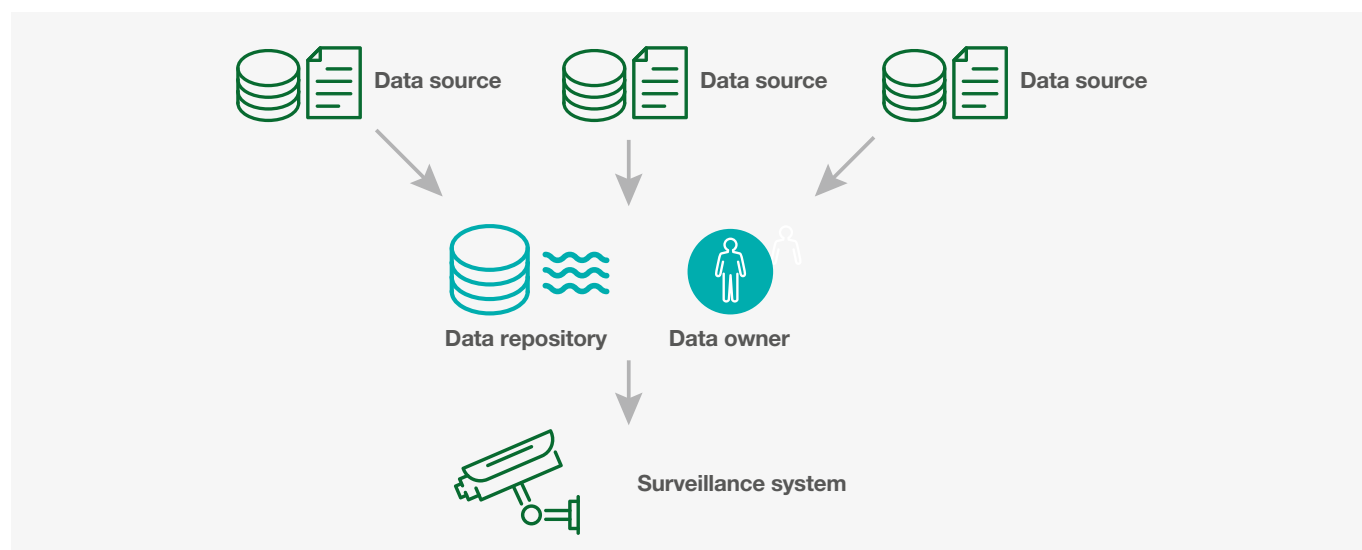


Figure 3: **High level diagram of data flow with common data repository**



The above diagrams provide a high level illustration of data flows with and without a central data repository and how that could affect the number of parties responsible for data quality. It is noted in reality that data flows are significantly more complex.



3.4 Current data quality control frameworks

What are the current state challenges?

Most firm's surveillance functions have controls in place to assess the CAT of data ingested into surveillance systems, however these controls often do not cover the entire data journey from original source to ingestion.

These controls may be automated or manual.

- Completeness controls are used to confirm completeness of surveillance data from upstream sources, comparing the count in both systems to confirm they match.
- Accuracy checks are in place to confirm the critical data elements required for surveillance are present.
- Timeliness controls monitor the delivery of surveillance data in line with agreed Service Level Agreements (SLAs). For example, for communications surveillance, data consumers may have automatic flags if a data feed has not arrived for ingestion by a specified time.

In many market abuse risk assessments, there is a failure to adequately consider the CAT of the underlying data. While firms diligently assess inherent and residual risks based on the models deployed within the surveillance system and other compensating controls, they often fail to articulate how data quality issues can undermine the effectiveness of these models and controls, leading to an overly optimistic view of residual risk exposure.

This lack of reference to foundational data quality can have significant consequences: overstated control effectiveness, understated residual risk, and ultimately, an increased risk of failing to detect potential instances of market abuse. By neglecting to assess CAT of data feeds as part of their risk assessments, firms risk building their surveillance programmes on an incomplete foundation, leaving them vulnerable to significant financial, regulatory, and reputational damage. Firms should consider integrating data considerations into their market abuse risk assessments, thereby ensuring that data quality is not an afterthought, but a central pillar of their risk management framework.

“Firms should consider integrating data considerations into their market abuse risk assessments, thereby ensuring that data quality is not an afterthought, but a central pillar of their risk management framework”



3. Data management and governance

Key considerations for how firms can address current state challenges

Firms could consider adding the following CAT controls to their critical data elements for surveillance.

Completeness controls check that surveillance-relevant data includes the values and types of data it is expected to contain, including any metadata that should accompany the datasets. The completeness control monitors the completeness of surveillance data by comparing record count between source system and destination systems for the data feeds.

- Record reconciliation – reconcile daily trade and communications volumes captured by upstream systems with those ingested by surveillance. Discrepancies would point to missing data.

The accuracy control checks the accuracy of surveillance data transferred between source system and destination.

- Matching/cross field validation – reconcile records with the upstream feed(s) and highlight fields that have not matched.
- Outlier detection – identify critical data elements that deviate significantly from the rest of the dataset. Outliers could suggest data corruption.
- Data type check – review the critical data elements conform to the expected schema.

The timeliness control tracks delivery of the dataset against the defined delivery time in Operating Level Agreements('OLA')/SLAs.

- OLA/SLA check – has dataset been received within the agreed OLA/SLA

Given the scale and breadth of data used across most firms, it would not be feasible or sustainable to run CAT controls manually, and therefore automatic reconciliations would be a more effective measure to gain comfort over the CAT of data.

We recognise that some firms' systems do not yet have embedded automatic reconciliations and suggest that this should be considered a target end state, whether this takes the form of upgrading to new systems or as additional features added to existing systems. For firms without system-embedded automatic reconciliations, additional automatic reconciliations, such as those described above, would be a useful measure to validate the CAT of data. We note additionally that the responsibility for operating these data quality controls will often fall outside of surveillance functions, for example, they may be operated by technology teams.






4. Opportunities for improvements in data quality

“You peel the onion back only to find another layer of issues”

4.1 Data sourcing and complexity

A challenge common for all firms is sourcing various data types and having confidence that the data captured is both complete and accurate. Whilst confidence and control over the integrity of entire data sets presents firms with a variety of problems, these firms also face specific challenges relating to the data once it has been successfully sourced. For example, order data can be particularly complex when looking at different types of parent and child orders. Challenges with data complexity for parent-child orders can exist for several reasons:

	Complexity and opacity	Parent-child order structures are often intricate, with child orders being spread across different times and prices making it more difficult for surveillance systems to identify underlying intent and potential market abuse.
	Abusive vs. non-abusive strategies	Parent-child strategies are an accepted and legitimate way of handling large orders; however, trade surveillance systems may struggle to distinguish between a legitimate strategy and an abusive activity such as layering and spoofing.
	Data latency and aggregation	For optimal monitoring, surveillance systems need access to the timing of all child orders to effectively monitor the parent order.

At times, it can be difficult to distinguish between legitimate trading practices and manipulative behaviours that, on the surface, can appear remarkably similar. This is particularly true when analysing activities like layering and spoofing, which can look similar to legitimate market making.

- Intent is the differentiator: while both market makers and manipulators engage in placing and cancelling orders, their underlying objectives differ significantly. Market makers aim to provide liquidity and profit from bid-ask spreads, while manipulators seek to create a false impression of market activity to deceive other participants and profit from artificial price movements.

Unexecuted Request for Quotes ('RFQs'), particularly those conducted through voice channels, present a unique set of challenges for surveillance teams tasked with identifying potential market abuse. These challenges arise from the difficulty in establishing a clear audit trail. Voice RFQs often lack a direct, time-stamped link to subsequent trades. This makes it difficult to track the flow of information and determine if the RFQ content was improperly used for illegitimate gain.

- Data capture and linking: capturing and linking RFQ data, especially from voice communications, presents significant technical hurdles. Linking voice recordings to specific instruments, trades, and timestamps requires sophisticated voice-to-text technology and data integration capabilities.

4.2 Non-standardised data

Non-standardised data can create challenges in detection, difficulties in data aggregation and analysis with data across various sources and increase false positives. Additional complexity arises via voice RFQs and Indications of Interest ('IOIs') which have tonal elements that are important to traders as participants are potentially communicating levels of interest and flexibility.

Over-standardising voice RFQ and IOI communications. e.g., by following a fixed script, risks losing the tonal element once ingesting the details into a voice to text solution, which is important in establishing trader intent to support effective monitoring.



4. Opportunities for improvements in data quality

4.3 Fragmentation of data and linking unstructured data to trades

“Like scattered pieces of a puzzle, Firms are dealing with fragmentation of communications data, with multiple pipes of unstructured data.”

Fragmentation of data makes it difficult to obtain a holistic view of trading activity, potentially allowing market abuse behaviours to remain undetected.

A specific example of data fragmentation is the difficulty faced by firms in matching unstructured communications data to trades. Currently, firms generally address this through manual trade reconstruction, and it has been indicated that it would take disproportionate levels of resource and investment to systematically link communications and trade data automatically. Trade data can often be organised in a pre-defined format with established fields for order details, information related to the financial instrument and timestamps, making it easy to search and analyse. Communications data is not generally organised in a pre-defined format. Integrating and analysing data types, which are so vastly different, requires sophisticated technology and methodologies which are not commonly deployed in the market.

4.4 Increasing regulatory expectations

“Regulatory scrutiny on firms who fail to effectively manage their data”

Firms noted that regulators have previously acknowledged that, due to the size and complexity of many firms, data quality issues are difficult to manage. However, there is now a sense that the grace period is over and scrutiny regarding data governance, ownership, and management is increasing. Regulators have demonstrated their interest in firms having complete data feeds, whilst identifying and rectifying data-based issues as quickly as possible. This increased scrutiny is starting to crystallise through recent enforcement actions and fines.

There are still challenges for firms in capturing all pre-trade data and remaining gaps in implementation of effective data controls. At present there is a clear risk of an expectation gap between what firms can achieve in practice versus what regulators may now expect. In addition to this, firms must adhere to additional requirements in relation to their third-party data providers, such as developing a third-party risk management framework that outlines how they will manage digital operational risks from their third-party data providers, as a result of the Digital Operational Resilience Act (DORA)⁴.

Key considerations for firms to enhance data quality

In conclusion, before firms can begin considering deploying holistic surveillance, utilising disparate data sets and machine learning, they must first address the foundational challenge of data integrity. Without confidence in the CAT of their data that meets a minimum accepted standard, any subsequent surveillance efforts are likely to be inherently flawed, leading to inaccurate risk assessments where residual risk ratings are overly positive, and a reduced ability to effectively detect market abuse. It is noted that data quality may never be perfect, and it is for firms to assess the quality of their own data before deploying more sophisticated technology. Firms should strive for improvements and enhance their capabilities iteratively once they have established confidence in the CAT of data.

⁴ For a list of suggested questions firms could ask third party data providers in order to gain comfort on the quality of data from third-party data providers, please see Appendix A



4. Opportunities for improvements in data quality

Firms could develop data mapping for market abuse behaviours, which would include:

- **Market abuse behaviour breakdown:** deconstruct each market abuse behaviour (e.g. front running) into its key stages and understand its behavioural steps.
- **Data requirement mapping:** for each stage of the behaviour, identify the specific data elements (critical data elements) required for detection, including their format, granularity, and source system.
- **Data repository mapping:** map the required data elements to the specific data repositories or systems where they are stored, both internal and external.

By doing so, firms will be confident in the completeness and integrity of required data capture to successfully monitor a market abuse behaviour. The mapping exercise provides a clear roadmap of the data journey, enabling firms to identify and address data gaps or inconsistencies that could affect their surveillance.

Below is an example for front running

Lifecycle of Trade/ Stage of Behaviour	Data Elements Required	Format / Granularity	Source System	Data Repository
1. Pre-Trade / Receipt of Client Order Information	<ul style="list-style-type: none">• Client order details (security, size, side, limit price)• Trader's access logs to order management systems• Communication records (emails, chats, voice)	<ul style="list-style-type: none">• Textual data• Timestamped access logs• Audio/text transcripts	<ul style="list-style-type: none">• Order Management System (OMS)• Communication Surveillance System	<ul style="list-style-type: none">• Centralized order book• Employee activity logs• Communication archive
2. Trade / Proprietary Trade Execution	<ul style="list-style-type: none">• Trader's trading account activity (orders, executions)• Market depth data (bid/ask prices, volumes)	<ul style="list-style-type: none">• Trade blotter data• Market data feeds	<ul style="list-style-type: none">• Trading Platform• Market Data Provider	<ul style="list-style-type: none">• Trade blotter database• Market data repository
3. Trade / Client Order Execution	<ul style="list-style-type: none">• Client order execution details (price, volume, time)	<ul style="list-style-type: none">• Trade blotter data	<ul style="list-style-type: none">• OMS	<ul style="list-style-type: none">• Centralized order book
4. Post-Trade / Profit Realisation (if successful)	<ul style="list-style-type: none">• Trader's trading account P&L• Market price movements	<ul style="list-style-type: none">• Account statements• Market data feeds	<ul style="list-style-type: none">• Back-office systems• Market Data Provider	<ul style="list-style-type: none">• Profit and loss database• Market data repository



5. Data ownership

5. Data ownership

Effective data ownership and governance is crucial to facilitating effective surveillance. Those that have issues with data governance will also likely have issues with surveillance controls such as alerts for key market abuse scenarios. For example, an alert model may not be running at full potential, which may be due to incomplete data and / or critical data elements due to issues with data ingestion or transfer, which in turn is a result of a lack of clarity in responsibility / accountability for data at different stages of the data lifecycle.

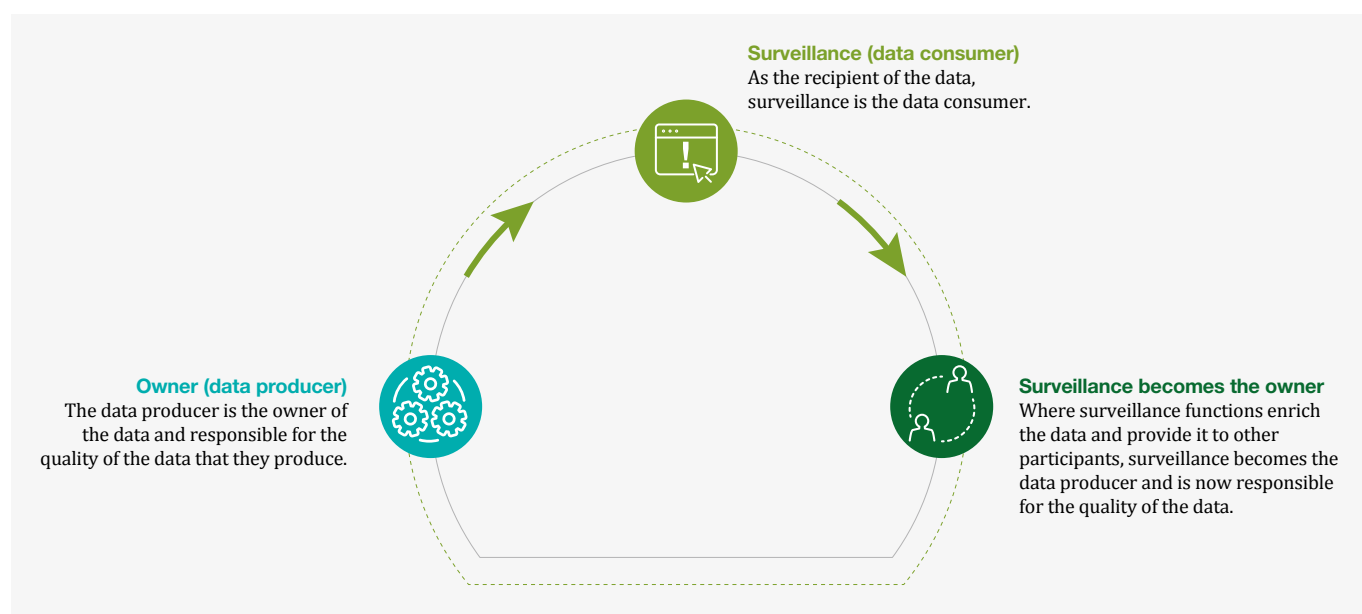
5.1 Ownership and current state

A common issue identified through the interviews was a lack of clear ownership relating to data governance. In general, the responsibility for data sits with the business, who produce vast amounts of data through trading activities, client interactions and market participation. However, Surveillance functions tasked with monitoring and analysing data from the business lack control over the data they consume and rely on. Without clear ownership and accountability, there is a lack of accountability for business units to prioritise data quality, leading to potentially ineffective surveillance and impacting the effective detection of market abuse. Clear ownership and accountability over the upstream data will enhance the detection of market abuse events.

5.2 Third-party data ownership & lack of industry collaboration

There is a growing view for third-party vendors and exchanges, who provide data to firms, to apply the same rigorous data governance standards that firms are expected to apply. For maximum effectiveness, the CAT of data needs to be validated and attested to at the beginning of the data collation process. In addition to this, firms may wish to align priorities and choose vendors that prioritise data quality and transparency as part of their business model.

Figure 4: **The flow of data between data producer and data consumer for surveillance**



Examples of issues observed with trading venue data sets:

- **Standardisation:** WebGUI data providers not including relevant fields within their activity report until requested by the client, even though the same fields were provided to other clients, using the activity report.
- **Completeness:** Trading venue not including quote messages within their drop copy data, even though the quotes can interact on the central limit order book (akin to an order).
- **Consistency:** Trading venue categorising an unexecuted immediate or cancel order (due to lack of liquidity) as a rejected order and not including the relevant price, quantity and direction in the rejection message within the drop copy.
- **Minimum Requirements:** Benchmark administrator not including order lifecycle information (enter, amend, cancel) or auction volume within their auction activity report.

5.3 What could good data governance look like?

Each firm will have a different business structure, however in general, best practice data governance would see the appointment of functional data officers responsible for performing data risk assessments, establishing data implementation plans where there are gaps and appointing data owners in line with a firm's bespoke data governance structure. Good data ownership governance includes a network of individuals responsible for data at different stages and these roles and responsibilities should be documented in a firm's data management policy.

It is critical that firms have clearly defined responsibilities as one of the most commonly flagged risks in our survey, as illustrated in the graph below, is the unexpected impact of upstream software and data schema changes. Clearly defined responsibilities would make it an individual's responsibility to identify their software and data schema changes, their downstream impacts and to help implement any required changes to mitigate consequential implications.

In some firms, we have also seen the appointment of a specific surveillance Data Guardian who is responsible for the controls that validate the completeness and accuracy of data feeds that are relevant for surveillance. This role is surveillance specific and involves interaction with more enterprise-wide data roles, like a divisional data officer, mentioned above, as well as reporting to relevant oversight forums and leading data forums and working groups. This allows surveillance to gain greater comfort that rigorous upstream controls are being performed and allow for more reliance on surveillance relevant data feeds.



5. Data ownership

Figure 5: **What are the top 3 risks that compromise the integrity of data for surveillance monitoring?**



The challenge of clear data lineage and ownership is often compounded by unclear responsibilities and siloed approaches to data management within firms. While surveillance teams are sometimes responsible for data quality "one hop" upstream (e.g., feeds from an intermediary data repository into surveillance), responsibility for data quality further upstream is often ambiguous. This lack of clarity is particularly pronounced for data originating from central data repositories used across multiple functions, such as market risk, finance, and regulatory reporting. Without clear ownership and accountability for data quality at each stage of the data lifecycle, the risk of errors, inconsistencies, and gaps propagating downstream to surveillance systems increases significantly. It is recognised as best practice for data producers to be responsible for the CAT of data, as outlined in section 2.

Key considerations for firms to improve data ownership

Firms should consider the following actions:

- **Data Inventory and Mapping:** conduct a comprehensive inventory of all data sources used for surveillance, documenting their origin, format, frequency, and intended use. This inventory should encompass all stages of the data lifecycle, from initial capture to aggregation and consumption by surveillance systems.
- **Data Flow Diagrams:** create visual representations of data flows, clearly illustrating how data is transformed, aggregated, and consumed by various systems and processes. These diagrams should highlight critical data quality checkpoints and clearly delineate data ownership and accountability at each stage.
- **Data Governance Framework:** establish clear roles, responsibilities, and processes for data ownership, quality assurance, and lineage documentation. This framework should foster collaboration and communication across organizational silos to ensure data quality is maintained throughout the data lifecycle.

By investing in data-related best practices firms can enhance their surveillance capabilities.



6. Surveillance data in practice

The below table provides an illustration of the key data elements that are required to detect a number of key behaviours, including spoofing, front running and ramping. The anticipated evolution of risk detection across these behaviours has also been summarised based on structured interviews across a subset of AFME member firms.

Behaviour / Importance of dataset in detecting risk	Considerations for key data elements that could be tracked (list of examples is non-exhaustive)	Evolution of key data elements to a Target state
Spoofing	<ul style="list-style-type: none"> • Timestamp of spoof order (order entry) / trade • Timestamp of cancellation • Order notional volume • Trade notional volume • Number of orders • Number of trades • Order / trade price • Order / trade type • Parties involved in the trade • Average daily trade volume • Communications data 	<ul style="list-style-type: none"> • Ability to capture voice orders in a timely manner • A shift from “alert to alert” to patterns / behaviours (e.g., order cancellation ratio) regarding client activity may involve building data repository (normal trend vs. not normal = trigger) • More effective cross venue / cross product detection to identify and detect this risk
Front Running	<ul style="list-style-type: none"> • Timestamp of order • Timestamps of trade and unwind trades • Order type • Order notional volume • Trade notional volume • Number of orders • Number of trades • Order price, execution price, unwind trade price • Asset / security information • Emails • Voice recordings • Instant messages • Market trading volumes 	<ul style="list-style-type: none"> • Better capture of RFQ data from third parties and voice RFQs, including those that are traded away • Better linkage / indexation between initial client contact to trade leading to front to back lineage of comms to trade • Better understanding of business profile information detection scenarios e.g., can pre-hedging risk be built into a surveillance tool reducing false positives
Ramping	<ul style="list-style-type: none"> • Timestamp of orders and trades (buy and sell) • Order price • Order notional volume • Trade notional volume • Number of orders • Number of trades • Emails • Voice recordings • Instant messages • Market trading volumes • Market price movement • P&L on the Large execution / cumulative large execution 	<ul style="list-style-type: none"> • Ability to monitor the “aggressiveness” or tonal elements of orders and identify who is positioning the orders • Advances to further develop the detection of cross product / market ramping. There needs to be more of a focus on this specific risk as it can be very beneficial and difficult to detect, an example of an area of concern is crypto futures vs crypto underlying • Firms would benefit from richer market data in less liquid markets, as well as bringing in further detail from various repositories, to improve monitoring • Similar to Spoofing, there needs to be a shift from “alert to alert” to patterns / behaviours



Summary of recommendations

To achieve the objective of enhancing data quality for effective surveillance in capital markets, a number of recommendations have been outlined as part of this paper. The table below provides a series of recommendations, which we previously discuss in this paper.

Topic	Section Reference	Recommendation
Poor quality data increases market abuse residual risks	→ Section 4: Opportunities for improvements in data quality	<p>Firms should now consider incorporating data feed completeness, accuracy and timeliness when reviewing the effectiveness of their controls and when assessing the residual risk for market abuse behaviours across products / business lines. This will lead to more informed residual risk ratings and will drive more effective and strategic surveillance solutions.</p> <p>Firms should also consider how confident they are in detecting market abuse behaviour and could consider incorporating data considerations to their market abuse risk assessments. For more information on data considerations, please see page 7.</p>
Knowing where your data is coming from and how it is being used	→ Section 3: Data management and governance → Section 5: Data ownership	<p>Surveillance functions should partner with business and/or IT functions to strengthen internal governance and to understand the sources of surveillance data flows, including any modifications or enhancements that are made to the data upstream.</p> <p>This should be documented as part of a data flow mapping, which is regularly reviewed and assessed.</p>
Lack of clarity in internal data ownership	→ Section 5: Data ownership	<p>Assigning ownership for data quality is crucial. This involves:</p> <ul style="list-style-type: none"> Identifying stakeholders accountable for completeness, accuracy, and timeliness of key surveillance data sources and feeds. Assessing the involvement of the surveillance function and determining ownership in cases of surveillance enriching data. Documenting roles and responsibilities in a data service level agreement and regularly review. Clarifying ownership of data from a Senior Manager Regime perspective.
Preventative and detective surveillance controls rely on a variety of data sources, viewed holistically, to drive insights	→ Section 4: Opportunities for improvements in data quality	<p>Firms should map market abuse scenarios to the relevant data points at each stage of the scenario to identify and retrieve the necessary data on a priority basis.</p> <p>Good quality surveillance controls rely on various data sources. Firms could identify these sources mapped to market abuse risks and focus on refining, reformatting, and transforming key data used for surveillance.</p> <p>Most firms have not sought to combine communications and trade data, which does not move the risk dial on all risks but may potentially facilitate better detection for risks such as front running. This should be a consideration once firms have got their data controls right for both communications and trade surveillance.</p>
Inconsistent governance standards amongst third parties	→ Section 4: Opportunities for improvements in data quality	Firms should assess third-party data providers against DORA principles, evaluating their compliance with data governance, quality monitoring, and lineage tracking.
Absence of common industry standards	→ Section 3: Data management and governance	<p>Firms should focus on increased collaboration and discussion of the current state of market and industry practices relating to data and improving data quality. Increased collaboration will also highlight common challenges and may promote innovative and holistic solutions.</p>



Topic	Section Reference	Recommendation
Data lakes / common data layers / repositories	→ Section 3: Data management and governance	<p>Firms should consider establishing a business owned central data repository that is recognised and maintained as an authorised data source. This would mitigate some of the risks associated with the various steps in the data journey from an upstream source into a surveillance tool.</p> <p>Surveillance teams must be highly confident in the CAT of the data they use. This could be supported by clear data sourcing documentation, and proactive engagement with data providers and the front office to ensure the data integrity of information feeding into surveillance processes</p>
Data quality control frameworks	→ Section 3: Data management and governance	<p>Firms should consider adding CAT controls to critical surveillance data elements.</p> <ul style="list-style-type: none"> • Completeness controls ensure data includes expected values and types, including metadata. • Accuracy controls verify data integrity during transfer between source and destination systems. • Timeliness controls track delivery against defined timeframes in agreements.
Key considerations for enhancing data quality	→ Section 4: Opportunities for improvements in data quality	<p>Firms should develop a data mapping for market abuse behaviours, which would include:</p> <ul style="list-style-type: none"> • Market abuse behaviour breakdown: deconstruct each market abuse behaviour (e.g. front running) into its key stages and understand its behavioural steps. • Data requirement mapping: for each stage of the behaviour, identify the specific data elements (critical data elements) required for detection, including their format, granularity, and source system. • Data repository mapping: map the required data elements to the specific data repositories or systems where they are stored, both internal and external.
What should good data governance look like?	→ Section 5: Data ownership	<p>Firms should consider the following actions:</p> <ul style="list-style-type: none"> • Data Inventory and Mapping: conduct a comprehensive inventory of all data sources used for surveillance and encompass all stages of the data lifecycle, from initial capture to aggregation and consumption by surveillance systems. • Data Flow Diagrams: create visual representations of data flows, illustrating how data is transformed, aggregated, and consumed by various systems and processes. These diagrams should highlight critical data quality checkpoints and clearly delineate data ownership and accountability at each stage. • Data Governance Framework: establish clear roles, responsibilities, and processes for data ownership, quality assurance, and lineage documentation. This framework should foster collaboration and communication across organizational silos to ensure data quality is maintained throughout the data lifecycle.



Conclusions and next steps

The responses to the surveys and deep dive interviews have identified a series of common challenges and current practices to firms' management of data and the impact of this on the effectiveness of Surveillance functions. This has supported the identification of key issues and recommended approaches, which collectively seek to act as a series of best practice principles.

In ensuring effective data management, firms will be able to deliver better surveillance outcomes, raise standards and operate more efficiently. We look forward to discussing our recommendations with key industry participants, as firms continue to develop and evolve their approaches in line with firm led initiatives and regulatory expectations.

“In ensuring effective data management, firms will be able to deliver better surveillance outcomes, raise standards and operate more efficiently”



Appendix A: Third-party data provider questionnaire

The below are designed to provide examples of questions which could be used to assess third-party data providers against the Digital Operational Resilience Act ('DORA').

Data governance

- Describe your data governance framework, including policies for data quality, security, privacy and lineage
- How do you ensure the completeness, accuracy and timeliness of the data you provide?

Incident management

- Describe your incident management process, including reporting and escalation
- What is your process for notifying affected data users of the incident?

Third-party risk management

- Do you rely on any third-party vendors for ICT services or data provision?
- If so, describe your third-party risk management framework

Data lineage

- How do you track the lineage of your data from source to client delivery?
- Can you provide auditable records of data transfers and transformation?

Independent audits

- Do you undergo regular audits of your ICT security and data management framework?



Appendix B: Surveyed challenges

Below are some examples that have been provided by AFME members of the types of challenges across the lifecycle of a trade in regard to data for effective surveillance.

Trade lifecycle	Challenges that if addressed can improve your surveillance effectiveness
Pre-trade	<ul style="list-style-type: none">• Capture of order data from third-party vendors (webGUIs)• Capture of all RFQ data for pre-trade resulting in trade or not• Lack of capture of IOIs data in any recorded medium because IOIs are expressed by the clients over voice• Incomplete data available and inadequate granularity from data source• Consistency between trade and order data• Segregated and multiple source systems or channels for trade and communications processing• Indexation of voice comms. Ability to quickly identify relevant conversation• Transform in labelled data Orders/RFQ (i.e. no STP between communication & capture system)
Trade	<ul style="list-style-type: none">• Reconciling quality of data provided by 3rd party provider• Occasional market data or trade feed delays from vendors (market-wide impacts)• Market fragmentation makes it more complex to ascertain all the data required. FX, Rates and Credit products remain more complex to monitor; and the data challenge is more pressing.• Unable to build controls around unrecorded devices leading to dependency on traders using recorded media. Additionally large false positive alert counts related to alerted unrecorded media lexicons.
Post-trade	<ul style="list-style-type: none">• Cross asset surveillance is a challenge for the industry; dynamic mapping of related instruments.• Linking comms to trades to conduct complete post-trade analysis is a manual process entirely• Data feeding timeliness, alert generation delay due to incomplete data.• Variation in timestamp data in different systems – primarily OTC activity e.g., IRS



/ 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 policymakers

Breadth

broad global and European membership

Pan-European

organisation and perspective

Global reach

via the Global Financial Markets Association (GFMA)



London Office

Level 10
20 Churchill Place
London E14 5HJ
United Kingdom
+44 (0)20 3828 2700

Brussels Office

Rue de la Loi, 82
1040 Brussels
Belgium
+32 (0)2 883 5540

Frankfurt Office

Große Gallusstraße 16-18
60312 Frankfurt am Main
Germany
+49 (0)69 710 456 660

Press enquiries

Rebecca O'Neill
rebecca.oneill@afme.eu
+44 (0)20 3828 2753

Membership

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

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

