

Data challenges for surveillance

Key insights

July 2025



Key challenges include maintaining accurate trading venue inventories, having an end-to-end data quality framework in place and applying a robust model risk management framework across surveillance scenarios. This paper outlines these challenges and how KPMG can assist firms in addressing them.

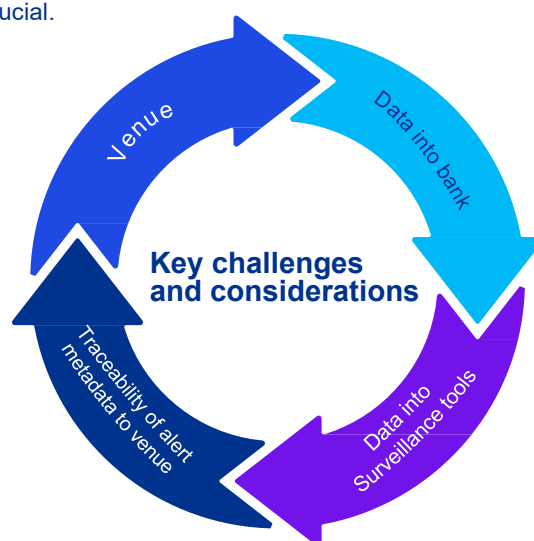
Navigating data challenges in surveillance: Ensuring quality and compliance

There is significant regulatory pressure on firms to capture pre-trade and post-trade data, and to ensure data quality - whether data is sourced internally or externally from third party vendors.

Poor data quality leads to ineffective surveillance controls compromising ability to detect market abuse risks. This could compromise market integrity, cause reputational damage for firms, and result in large regulatory fines.

Firms must enhance data quality for effective surveillance

Firms need complete, accurate, and timely data to effectively detect market abuse. Establishing a robust data quality framework through implementing effective governance, controls and comprehensive policies and procedures is crucial.



Potential output: models/datagaps

Data challenges are preventing firms from surveilling effectively

Data challenges are significantly hindering firms' ability to conduct effective surveillance. The key issues are outlined below:



Comprehensive venue inventory/ venue risk assessment

Firms struggle to collate and maintain a complete and accurate inventory of trading venues. Without a clear methodology for venue risk assessment, firms will struggle to identify and mitigate risks associated with trading on specific venues. Firms should implement a robust risk assessment methodology, including logging key venue attributes and prioritizing high-risk venue attributes based on historical enforcement cases.



Data quality (completeness, accuracy and timeliness of data)

Most firms' surveillance functions have controls in place to assess the quality of data ingested into surveillance systems, however these controls often do not cover the entire data journey from original source to surveillance, often due to fragmented data architecture. Issues with data quality could result in gaps in surveillance, which in turn could result in missed filings of market abuse to the regulator.



Data traceability/capture of venue attributes

Firms face challenges capturing venue information within their alert metadata. The traceability of metadata back to a venue is an important factor in demonstrating venue governance. However, complex data structures, as well as filtering logic between upstream systems makes this challenging for firms to achieve.



Model risk management (MRM)

The application of a model risk management framework over surveillance scenarios, remains an area of challenge for some firms. A robust MRM framework can support with bolstering the data quality framework. For example, independent validation may identify potential data gaps due to errors in the underlying design or logic of the surveillance scenario.



Data sourcing, governance and ownership

Without a clear line of sight for all relevant data sources, it is difficult to assess the completeness of data coverage. There is often a lack of clarity of ownership regarding who is responsible for the quality of data flows from internal upstream sources, which can be multiple 'hops' from when the data is utilised in the surveillance system. It is important for firms to have visibility of their front to back system cartography, including the definition of key data elements that are required from source system to surveillance. Failure to gain this understanding results in difficulties when applying ongoing governance over data.

How KPMG can help

Surveillance experience and expertise

KPMG brings a combined experience in market abuse regulation, surveillance and data analytics. We have supported various banks through surveillance data quality, venue risk assessment as well as reviews, venue risk assessments as well as data quality remediation.



Venues risk assessment/venue inventory

We have a defined methodology to support firms with undertaking a venue risk assessment. Our methodology helps firms with the capture of key venue attributes, as well as the mapping of these attributes to expected market abuse behaviours. This allows firms to not only maintain an effective venue inventory but also create linkage between the venue inventory and the market abuse risk assessment.



Assessment of data management framework

We have helped firms with reviewing and updating their data flow cartography in order to address the data sourcing challenge and help validate external data sources. We can also support with enhancing data controls, including completeness, accuracy, and timeliness standards - as well as testing them. Additionally, we can review any filtering and data logic & validation processes to ensure that data is correctly processed and interpreted.



Data traceability/gap assessment

We can help with conducting a gap assessment across systems to ensure comprehensive data traceability and a front to back view of end-to-end data inputs. This allows firms to know what they are missing and have visibility over whether the data is complete, accurate and timely. This ensures that all relevant data is accurately recorded and traced, enhancing the firm's ability to monitor and respond to potential market abuse effectively.



Alerts review lookback

We have extensive experience supporting banks with operational planning and execution of lookback alert review exercises. This includes formulating a plan for dispositioning a defined population of trade surveillance alerts, understanding the risks associated with each in-scope alert types and supporting with QA. We have the knowledge and expertise to perform trade surveillance alert reviews, investigations, and escalations in line with a firms' procedures.



Surveillance model validation

We also have a strong model risk management team that understand the MRM framework and regulatory standards which need to be applied to model use and performance. Combined with our deep expertise in market abuse surveillance, we can support with the independent review and validation of surveillance models.

Case studies



Surveillance Model Evaluation – Major Global Bank

A major global bank committed to the Fed to enhance its model risk governance framework. The bank needed a partner to independently assess all submitted models against new criteria. Surveillance models have been on boarded to the model risk management framework for the first time.



Venue Metadata Analysis – Global Investment Bank

A major global investment bank required a current state assessment reflecting the bank's ability to tag existing trade surveillance metadata back to their underlying trade venue and a roadmap to remediating any gaps.



Alert Review Backlog – Global Investment Bank

Provided support to a global investment bank to remediate and optimise their monitoring and surveillance processes, covering the relevant areas in the investment bank, with the inclusion of a surveillance alert lookback strategy and execution. This involved developing a process to review alerts for certain scenarios and products for over 60 thousand alerts



Data Quality Controls Testing – Global Investment Bank

A major global investment bank subject to a consent order required a front to back review of data quality controls. The review covered various surveillance capabilities including trade, communications, and unauthorised trading.



Venues Risk Assessment – Global Investment Bank

Supported a global bank with establishing their venue risk assessment methodology. This included consideration of key data fields for establishing a venue inventory, prioritisation of venue attributes and the mapping of key attributes to associated market abuse behaviours.



Scenario Recertification – Global Investment Bank

A major global investment bank was required to reinforce their controls framework to ensure surveillance completeness. The outcomes were:

- Validated data completeness and accuracy e.g. inventory upstream feeds, transactions, exclusions.
- Confirmed data availability for surveillance monitoring e.g. 'greenlight' thresholds to confirm data availability for surveillance.
- Documented data lineage from source systems to the final output control systems.
- Bolstered the overall surveillance set up e.g. reprocessing/lookback capabilities.

Contact us:



Lucas Ocelewicz

Partner

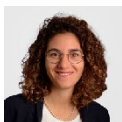
lucas.ocalewicz@kpmg.co.uk



Dharam Shah

Director

dharam.shah@kpmg.co.uk



Joy Chetrit

Senior Manager

joy.chetrit@kpmg.co.uk

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

kpmg.com/uk



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.

© 2025 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Document Classification: KPMG Public

Create | CRT162812A | July 2025