Protecting against market abuse and misconduct risk

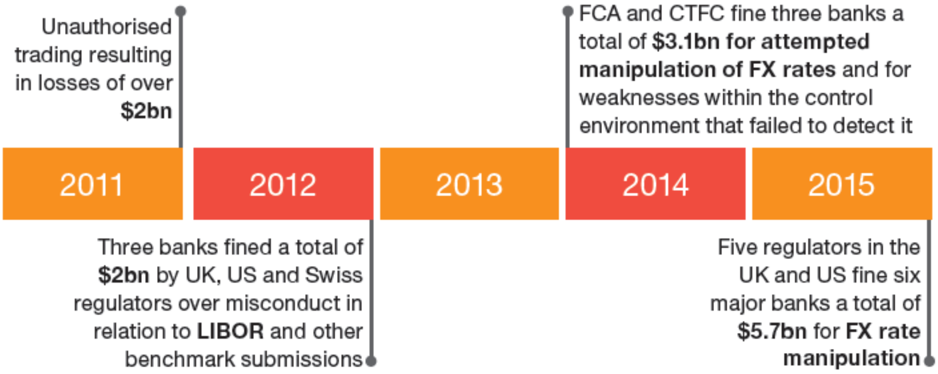
A holistic approach to surveillance

Our approach to surveillance is based on helping numerous financial institutions respond to regulatory inquiry or sanction and working with those clients to avoid future violations

B2B SALES STRATEGY & BRAND COMMUNICATION
SALES STATS
BRAND IDENTITY

Background

In the last five years, financial institutions have incurred losses from rogue trading incidents, and have been investigated and fined over allegations of rigging foreign exchange markets and other market abuses



2011

Unauthorised trading resulting in losses of over **$2bn**

2012

Three banks fined a total of **$2bn** by UK, US and Swiss regulators over misconduct in relation to **LIBOR** and other benchmark submissions

2013

2014

FCA and CTFC fine three banks a total of **$3.1bn for attempted manipulation of FX rates** and for weaknesses within the control environment that failed to detect it

2015

Five regulators in the UK and US fine six major banks a total of **$5.7bn** for **FX rate manipulation**

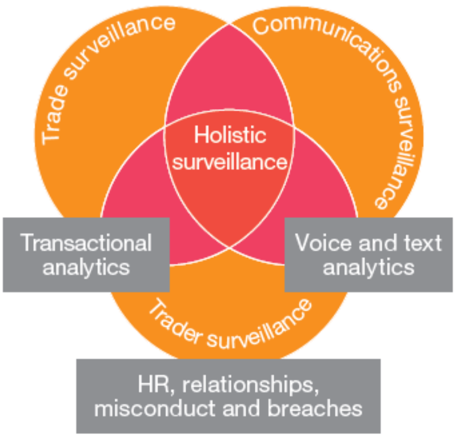
At the heart of the benchmark manipulation scandals has been the use of chatrooms, instant messaging and email to enable collusion between traders. The use of electronic communication to engage in collusive behaviour has led to increased scrutiny around how financial institutions monitor and control their communications, and how misconduct can be detected using trader surveillance.

As a consequence, the regulatory landscape for surveillance is changing. In addition to the existing FCA market conduct rules and EMSA guidance on real time monitoring, MiFID II and other planned regulation will have an impact on how firms monitor and report on their trading activity and trader behaviour.

Surveillance is becoming increasingly sophisticated, with global regulators having an increased expectation that institutions will conduct holistic surveillance over multiple data sources including trade and order data, electronic and voice communications, and behavioural data in order to identify potential market abuse and misconduct.

We bring expertise and insight into the tactical and strategic solutions that support the Financial Services sector's growing surveillance requirements. We have worked across a wide range of financial institutions, helping them with their investigations and responses to requests from regulators, and also with their forward looking surveillance solutions.

Definitions of surveillance



Considerations in developing a surveillance capability

Developing an enhanced surveillance capability is challenging but also provides opportunities.

There are a number of considerations which we believe help determine what surveillance capability is right for you:

- What level of monitoring and surveillance do you need and where within your organisation will responsibility for it lie?
- There are many surveillance vendor solutions available, or you can build your own. How do you make the right technology decisions to support both tactical needs and strategic vision?
- Behavioural analytics is widely perceived as the future of surveillance. What does it mean to you?
- For many financial institutions the increasing costs of electronic communication ('e-comms') surveillance are a concern. Can you optimise search strategies, make lexicons more effective and reduce false positives?
- How confident are you in your data capture, archiving and retrieval processes?

This folder sets out the key elements of a successful holistic surveillance solution and our approach to implementing them.

Organising your surveillance capabilities

Surveillance target operating model

How do you define surveillance?

Who owns and is accountable for surveillance?

Is surveillance combined across business divisions?

Will surveillance be managed and applied globally or regionally?

How do you define the role of the Front Office and Compliance with respect to surveillance?

How do you minimise duplication of effort and increase efficiency?

How do you make decisions on your long-term technology partner?

Regulatory pressures and changes within the industry

The regulatory landscape for surveillance is changing in response to recent high profile events in the Financial Services sector. Regulators increasingly expect financial institutions to have sufficient surveillance capabilities to cover all regulatory scenarios, incorporating an increased number of data sources and communications channels.

As a consequence, surveillance procedures and controls have become increasingly important for financial institutions. Many industry participants are evaluating whether their current surveillance operating model is fit for purpose and deciding upon the level of investment required to manage the business risks to within their appetite.

Your surveillance operating model needs to be proportionate to your requirements which will depend on both the businesses you have and the jurisdictions you operate in. These differences means that there is no ‘right answer’ and it can be hard to know what will suit your needs.

Emerging operating models

The regulatory direction of travel encourages a ‘new normal’ for the surveillance operating model, which suggests, but does not prescribe, that surveillance responsibilities are allocated across the lines of defence (‘LoD’s). Many financial institutions are therefore considering the extent of 1LoD and 2LoD mandates for surveillance to ensure an appropriate balance of surveillance activity. The development of the Senior Managers and Certification Regime will also influence the balance and injection of surveillance activities across the lines of defence.

Our expectation is for the 1LoD surveillance tools to be sufficiently calibrated to capture business critical issues that present a significant operational risk to the financial institutions, while the 2LoD would be responsible for monitoring compliance with regulatory rules, internal policies and controls. The 2LoD has to be independent from the 1LoD and use surveillance techniques to support monitoring efforts, for example identifying and developing risk based surveillance scenarios that can be run across asset classes.

Emerging operating models

Emerging 1LoD surveillance functions

Model 1: Front Office supervisory team

Separate teams have been established in the Front Office that are responsible for creating, maintaining, supporting and enforcing the Front Office supervisory control framework. This team acts as a conduit for passing information to the supervisor, and subsequently holds the supervisor to account by monitoring the completion of surveillance activities by the supervisor.

Model 2: Front Office risk and controls team

This model establishes a level of independence within the 1LoD, with a separate team responsible for conducting Front Office surveillance activities. Results of surveillance activities will be closed down or escalated to Front Office supervisors for their independent review and decision.

2LoD surveillance functions

- The 2LoD Surveillance Function resides within Compliance and is independent from the 1st Line.
- 2LoD surveillance activity is driven by regulatory requirements, internal standards and responding to emerging market issues.
- The 2LoD Surveillance Function will own and build independent scenarios to identify instances of unusual trading patterns, or communications (both electronic and voice).
- The 2LoD will review and escalate any unusual findings to relevant committees and other functions for onward investigation.

Our approach

We have developed an approach to support financial institutions with reviewing, designing and implementing their surveillance operating model. Our framework identifies both the key areas for surveillance and the surveillance capabilities required to protect and provide the financial institution with a level of confidence that it is operating in accordance with relevant regulatory requirements.

Regulation

Existing regulation and other regulatory drivers, such as the requirement to provide attestations, will identify a core set of requirements for surveillance. We can draw on our global team to provide a view on regulatory expectations in your key locations.

Risk identification and assessment

We can support you with defining and prioritising the key risks you manage across asset classes. Those risks may apply globally, across lines of business, or may be very specific to a particular region or asset class. We will work with you to understand your governance framework, geographic reach, market profile and policy framework to determine your surveillance requirements.

High level surveillance operating model

We can support you to develop a target surveillance operating model, which considers the establishment of governance forums, the allocation of roles and responsibilities, technology and data requirements, key business and functional requirements and integration with existing institution-wide processes. Once designed, we can support you in undertaking a gap analysis and implementing the programme of work required to roll out the model across relevant locations and divisions.

Review and enhance operating model

We can also assist you with reviewing your existing model in order to make it more efficient and effective, including the implementation of centres of excellence.

Credentials

We were asked to help a large financial institution make an informed decision on what its trade and sales surveillance capability and operating framework should look like.
The client requested an analysis of its current state, a global view of regulators' expectations in this area, an overview and shortlist of possible surveillance technology, and insight into how other banks are approaching the subject.

Using our expertise in trade and e-comms surveillance we provided analysis of key choices available within the client's high level operating framework for trade surveillance, including potential impact on 1st and 2nd line monitoring functions. The client is using our report to inform key decisions within the Compliance function of the bank.

What PwC can offer you

Experience

We bring a breadth of experience from both designing surveillance operating models and implementing surveillance frameworks within large financial institutions.

Tailored designs

We recognise that each client has different capabilities, cultures and demands for which an operating model must fit. We recognise the balance of tailoring the design to be most effective for the shape of your business whilst ensuring its ability to meet global regulatory expectations.

An independent, trusted advisor

We act as a trusted advisor, providing an independent perspective based on our experience building operating models for other financial institutions.

Navigating the surveillance vendor landscape

Surveillance vendor evaluation

Are my planned surveillance capabilities sufficient to meet evolving regulatory expectations?

What is evolving industry practice and what has been the experience of other financial institutions?

Which vendor solutions best fit with my surveillance operating model?

Which surveillance solutions integrate the best with my IT environment?

What level of analytics sophistication is the firm comfortable with for its surveillance platform?

Regulatory pressures and landscape

Surveillance is a priority issue for many financial institutions, as global regulators push for a higher degree of monitoring of Front Office sales and trading activity in light of recent investigations into the manipulation of LIBOR and FX benchmarks. Regulators increasingly expect financial institutions to have a surveillance capability which covers all asset classes across all regulatory scenarios and which incorporates all data sources and communication channels available. Financial institutions are starting to develop such surveillance across asset classes and locations, to embed a consistent surveillance model across their businesses.

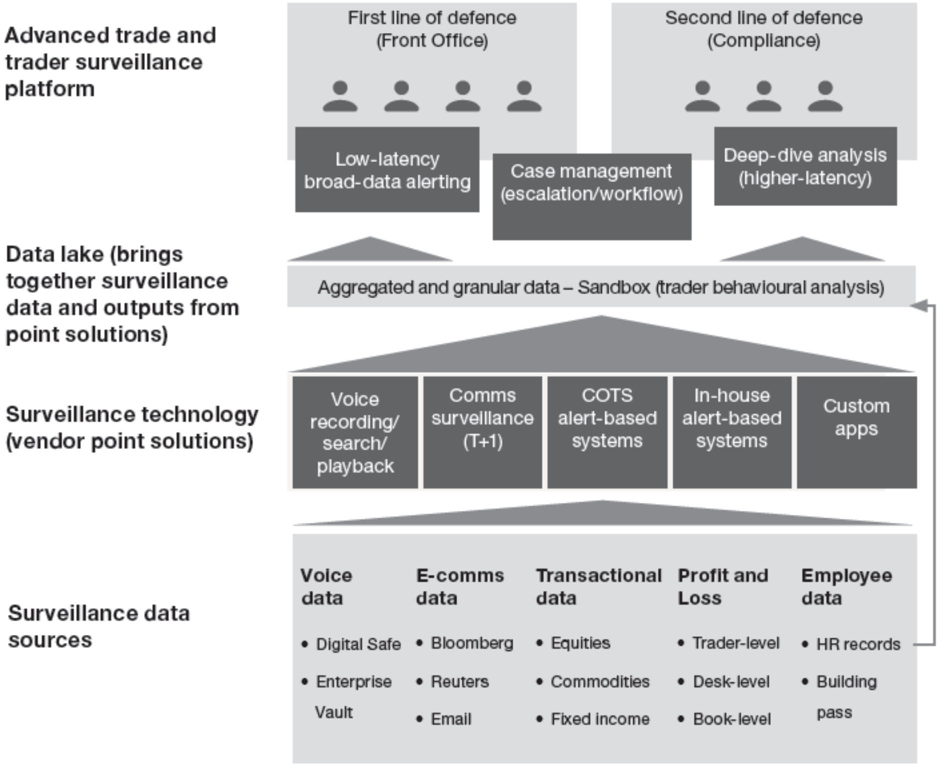
Surveillance technology vendor landscape

In response to increased regulation we have seen a proliferation of software vendors offering surveillance solutions. There are a number of new entrants challenging the traditional options.

The vendor landscape is fragmented and predominantly consists of solutions that focus on a distinct specialism such as voice communications, electronic communications, or transactional data, with only limited ‘joining of the dots’ or triangulation between the data points. In addition, vendor solutions frequently have different approaches, architecture and algorithms, and interact with the financial institutions’ various systems differently.

The schematic below represents our view of emerging surveillance practice which requires the integration of multiple data sources and potentially vendor solutions. Consequently, navigating the vendor landscape is a complex undertaking.

Emerging surveillance practice


Advanced trade and trader surveillance platform
First line of defence (Front Office)
Second line of defence (Compliance)
Low-latency broad-data alerting
Case management (escalation/workflow)
Deep-dive analysis (higher-latency)
Data lake (brings together surveillance data and outputs from point solutions)
Aggregated and granular data – Sandbox (trader behavioural analysis)
Surveillance technology (vendor point solutions)
Voice recording/ search/ playback
Comms surveillance (T+1)
COTS alert-based systems
In-house alert-based systems
Custom apps
Surveillance data sources
Voice data
• Digital Safe
• Enterprise Vault
E-comms data
• Bloomberg
• Reuters
• Email
Transactional data
• Equities
• Commodities
• Fixed income
Profit and Loss
• Trader-level
• Desk-level
• Book-level
Employee data
• HR records
• Building pass

Our approach

PwC has built up a detailed knowledge of the surveillance vendor landscape. We have investigated rogue trading incidents, LIBOR and FX market manipulation, and we have used the knowledge we have gained from these to work closely with Front Office and Compliance functions to understand market abuse and how to detect it. Leveraging this experience and insight we have developed a trade surveillance technology assessment offering to support financial institutions with their vendor evaluation and selection process. We can help you navigate the vendor landscape and select technologies appropriate to you.

Our assessment approach:

Information collection and market review

We work with you to articulate your requirements. The ‘use cases’ we develop provide an effective means of assessing initial levels of vendor fit to your organisation.

Scorecard development

We assess each vendor solution applying criteria which cover both functional and non-functional requirements, and the degree of fit to your business and IT landscape.

Vendor profiling

We provide a detailed assessment of each vendor and how well their solution fits your specific needs.

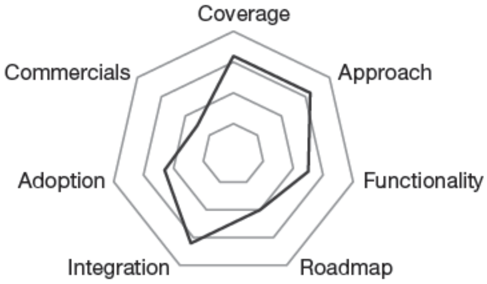
PwC evaluation

We can run proof of concepts, using your data, or syndicated data, to establish the performance of the vendor software. We bring objectivity and provide rigorous examination of vendor capability. We have pre-built scorecards and evaluation criteria.

Easy to interpret analysis

We provide intuitive outputs from our analysis to ease interpretation and provide a clear basis of comparison between different solution options.

Vendor A – Illustrative



Highly mature compliance monitoring tool which enables all surveillance functions for electronic communications. A strong support organisation and highly experienced with all comms channels excl. voice. Potentially a strong option for integration with a market abuse transaction monitoring tool.

Credentials

We recently supported a large international bank by providing market analysis of trade and e-comms surveillance providers and technologies. We provided an overview of regulators’ expectations regarding sales and trade surveillance, including recent key developments, current issues, and our assessment of how expectations are likely to develop in the medium term in our client’s key locations.

Using our expertise in trade and e-comms surveillance we provided analysis of key choices available within the bank’s high level operating framework for surveillance, including potential impact on 1st and 2nd line monitoring functions.

What PwC can offer you

Regulatory insight

Our global network of firms contains subject matter experts with knowledge of how regulators’ thinking in your key territories is developing. We can use our network to support your assessment around which technology options will help you meet developing regulatory expectations.

Industry insight

We work with many of the largest global banks on sales and trade surveillance related matters and as they build surveillance capabilities across their UK, US and Asia Pacific offices. We can leverage our understanding of peer banking practices to provide insight into your key technology options.

Technical insight

We work with a number of the key technology providers in the sales and trade surveillance space and have been closely involved in detection and reporting of inappropriate sales activity, insider trading, rogue trading and benchmark manipulation for major global banks. We can apply our experience to assist with your proactive monitoring and surveillance solution assessment.

Targeted analysis

We have developed tools to provide easy to interpret analysis to show differences between different solutions, and we have a proven track record of delivering our services which enables you to progress your trade surveillance plans with confidence.

The future of surveillance

Behavioural analytics

What are the key risks I need to monitor for?

What data sources do I have available to support surveillance?

How do I develop the risk rules to detect misconduct and other risks?

How can I integrate structured transaction data with unstructured e-comms data to better detect risk?

How does behavioural analytics work and can it really identify issues of concern and at the same time reduce volumes of false positives?

The changing environment

Perhaps the greatest challenge arising from traditional surveillance activity is the volume of alerts and responses generated. How do you separate the true positives from the false positives with confidence?

Regulators' focus on conduct, defining conduct and how it is managed within financial institutions has encouraged senior management to be more dynamic with the way that single points of data are reviewed.

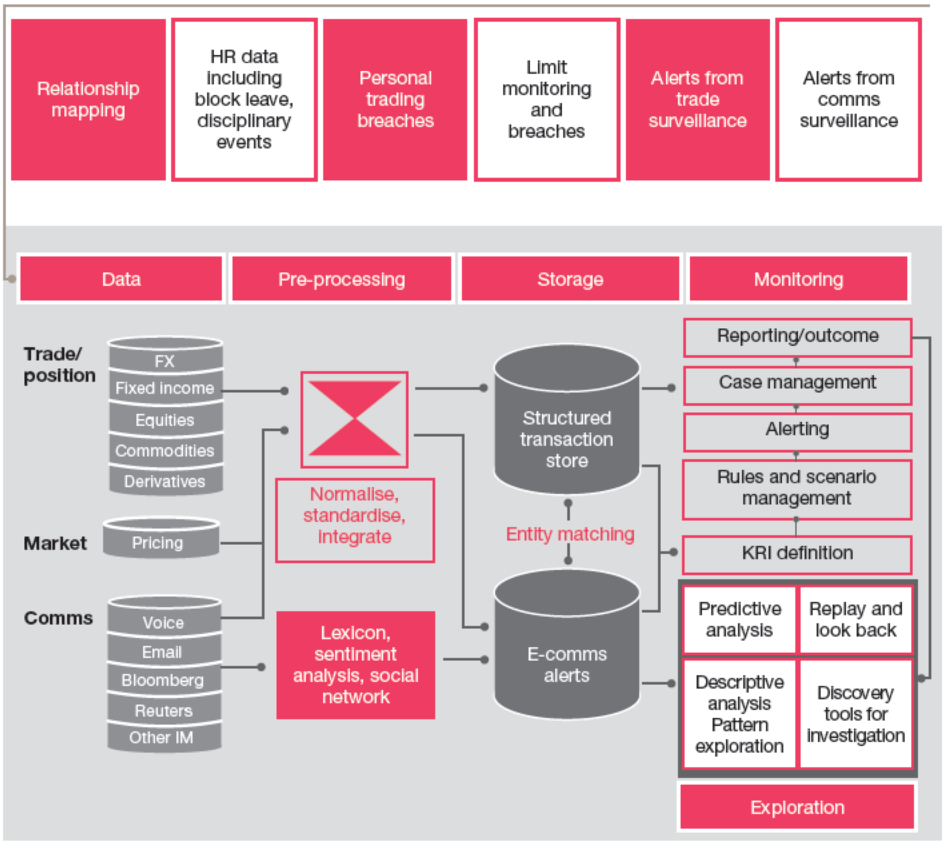
The use of behavioural analytics to support surveillance activities is based around two fundamental concepts:

- triangulation of data from multiple sources to enable a holistic view of trading activity; and
- using this data to look for anomalies or unusual patterns within the data.

Specifically, the algorithms applied look for differences in trader behaviour against both individual base line and peer group patterns of behaviour exhibited by individual traders. This brings a greater level of sophistication to the alerts and subsequent investigation process.

In order to harness the power of behavioural analytics, financial institutions need to consolidate their existing data sources, define the parameters for good and bad behaviour and aggregate alerts from 'point solutions' to home in on the areas of greatest risk.

Potential data sources for behavioural analytics


Relationship mapping
HR data including block leave, disciplinary events
Personal trading breaches
Limit monitoring and breaches
Alerts from trade surveillance
Alerts from comms surveillance
Data
Pre-processing
Storage
Monitoring
Trade/ position
FX
Fixed income
Equities
Commodities
Derivatives
Market
Pricing
Comms
Voice
Email
Bloomberg
Reuters
Other IM
Normalise, standardise, integrate
Lexicon, sentiment analysis, social network
Structured transaction store
Entity matching
E-comms alerts
Reporting/outcome
Case management
Alerting
Rules and scenario management
KRI definition
Predictive analysis
Replay and look back
Descriptive analysis Pattern exploration
Discovery tools for investigation
Exploration

Our approach

While trade and electronic communication ('e-comms') surveillance have traditionally been regarded as separate activities, effective surveillance increasingly requires trade and e-comms surveillance to be combined in order to reveal patterns of anomalous activity. Bringing together e-comms and trade data, to develop a unified view of trader activity and provide better triangulation of data sources to identify risk, involves significant data integration challenges, the use of advanced analytics techniques and a sophisticated alerting, case management and escalation process.

We apply behavioural analytics to both historic investigations and to support our clients' ongoing surveillance activities. In addition to triangulating trade and e-comms data, we increasingly factor in additional sources such as HR records, building pass swipe data and log in history to build a more complete picture of trader activity and to better identify instances of anomalous behaviour.

Understand requirements and potential data sources

We work with you to understand what your appetite for surveillance is, the risks identified within the business and the data available to support behavioural analytics.

Build profiles of trader behaviour

We create a 'sandbox' environment and profile data to determine behaviours.

Build algorithms to detect changes in trader behaviour

We apply predictive and descriptive analytical techniques to establish patterns of behaviour.

Improve monitoring performance

We track the ability of our analytical techniques to identify anomalous behaviour, and incorporate the outputs into our clients' surveillance solutions and existing rule sets.

Credentials

We have supported a number of clients in responding to regulatory requests regarding potential manipulation of benchmarks. We are able to ingest, explore, model and visualise multi-year trade and e-comms data to provide clients with a clear picture of their traders' trading activities across specific dates. We also provide a 360° view of traders and develop profiles of trading behaviour, utilising analysis of a wide range of trading patterns.

What PwC can offer you

Experience based analytics

Our analytical approaches have evolved out of investigations into real-world market abuse and rogue trading cases.

Analytically robust approach

We apply best of breed analytics techniques from predictive modelling, machine learning and data mining when developing our behavioural models.

Pragmatic industry insights

Our analytics team works closely alongside our industry and regulatory experts, ensuring our technical approaches remain pragmatic and focused on industry specific issues.

Vendor independent analytics

Our analytics approach is vendor independent. We have used a variety of vendor products in the past for surveillance analysis, but believe the most important success factor for behavioural analytics is the approach, rather than choice of vendor solution.

Minimising false positives, maximising the right alerts

E-comms and voice analysis optimisation

How do I increase the relevance of my search lexicons?

What is the most efficient way to review responsive items?

How do I undertake an effective review of voice data?

How can I use other data sources or techniques to increase the effectiveness of e-comms review?

How can meta-data analysis support the review strategy?

Electronic communications

Monitoring of electronic communications (‘e-comms’) and voice communications are becoming increasingly important components of an effective surveillance capacity.

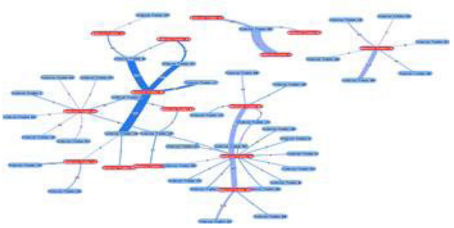
A key challenge faced by financial institutions is how to refine lexicon-based search techniques to target communications of interest. Key word search approaches are highly dependent on the quality of the lexicon used.

The use of key word and key word cluster searches is well established in automated surveillance over e-comms. Voice-to-text surveillance software uses the same principles to automate some of the surveillance function’s work, by triggering alerts when sus`picious words or combinations of words are used by the Front Office staff. Automated voice surveillance has the additional challenges of audio quality and accents. It is also more onerous to review, irrespective of whether phonetic or transcription techniques have been applied.

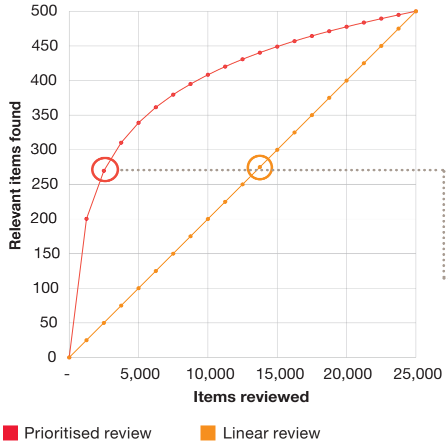
The consequences of high numbers of false positives generated by lexicon-based surveillance tools is an increase in the work effort and size of communication surveillance review teams. This in turn leads to concerns over the effectiveness of the review, and whether the reviewers in the first or second lines of defence have the requisite skills and experience to find the more subtle instances of market abuse.

The challenges for efficient review

Financial institutions are grappling with the challenge of whether to review all responsive Instant Messaging communications or to only review a sample. Vendor solutions provide the ability to review all e-comms. Analysis of all e-comms will have a consequent effect on the size of the review team required. Analytics can be applied both to optimise lexicons and also to drive review efficiency. We can apply meta-data analysis in combination with advanced analytical techniques to model who talks to whom, at what times of the day and how many participants are involved in the conversations. Application of social network analysis to identify interactions can be used to drive a targeted review strategy.



We use Response Optimisation Curves (‘ROCs’) to measure the effectiveness of search strategies.



Through this analysis we can optimise which search terms to use to return the highest number of relevant items for further review and escalation.

Prioritised review
Search terms with higher historic relevancy rates are given more weight, leading to a higher proportion of relevant documents being found at the start of the review process.

Linear review
All search terms are treated as equally important.

In this example, the prioritised review returns 275 relevant documents from a population of 2,500.

However, a linear review would need to review 13,000 items to find the same number of relevant documents.

Our approach

Through our investigative work with financial institutions, including reviews of benchmark manipulation and other market abuse incidents, we have developed an approach to optimising the use of keyword searches. Whether the purpose is to detect inappropriate market behaviour or breaches of an internal code of conduct, we will be able to help you to apply analytical techniques to minimise false positives whilst achieving a level of effectiveness proportionate to the risk.

Understanding the volume and quality of data

We perform a document review and hold discussions with key stakeholders to understand the data capture process, the data volume and the quality of data.

- Are all relevant communication channels recorded?
- If voice-to-text is used, is the data quality sufficient for an effective review?
- What can you achieve through analysis of the meta-data?

Lexicon optimisation

We review your lexicons for both quality and completeness. Market abuse lexicon across all asset classes can extend to thousands of words and phrases. We use optimisation techniques to help identify the effectiveness of your lexicon and drive greater efficiency.

Predictive analytics and entity relationship mapping

We can help you bring greater intelligence to the e-comms and voice analysis review process. We can combine meta-data with predictive coding and concept cluster techniques to identify who commonly talks to whom, and about what. This can be highly effective in enabling a more targeted review.

Review outcomes

We can help you manage your ongoing surveillance costs by delivering efficient and effective e-comms and voice review, reducing your need for large review teams.

Credentials

We undertook a detailed review of a large financial institution's communication monitoring systems to help rationalise the communications data and review methodology. Our client wished to ensure that its stretched Compliance function was able to effectively monitor communications of individuals sitting within the Front Office. We provided review technology and experienced personnel to alleviate a backlog in un-reviewed communications. In addition, we defined and implemented a complete and accurate central consolidated data store to enable efficient searching and review going forward.

What PwC can offer you

Cost effective review

We can increase the efficiency of your senior review team or counsel, by using our nearshore specialist centre to create an efficient and effective hierarchical review structure.

Analytical efficiency

Work smarter not harder is the ethos behind our approach. Our statistical techniques ensure that we minimise the review effort required to achieve the necessary level of effectiveness.

Domain experience

We are experienced in reviewing communications between traders, and understand the challenges arising from trader specific language and communication behaviour. Consequently we have developed a variety of techniques to address these challenges and provide an effective review.

Contextual analysis

We use social network and statistical profiling techniques to provide reviewers with more context around the communications under review, and to enable the reviewer to understand the pattern of communication as well as individual messages.

Safeguarding your surveillance data

E-comms records management and retrieval

Which e-comms channels are in use across the organisation?

What are the data retention requirements for each e-comms channel?

What controls are required to assure the reliability of the e-comms data archive?

How do we assure audio capture quality?

How confident am I that all e-comms data is being captured and archived completely and accurately?

Financial institutions

Financial institutions use a wide range of electronic communication ('e-comms') channels and voice platforms across their business. These include multiple email instances, third party provided channels, internal instant messaging systems, trader turrets, conference lines and corporate mobile devices. A lack of robust IT controls can lead to failures in the records retention process, putting the business at risk of regulatory sanction, enforcement action and reputational damage if regulatory requirements for data retention are not met. As scrutiny of Front Office conduct intensifies, it is imperative that financial institutions establish robust control over their e-comms channels. We believe this will include the need to validate data archiving processes, identify opportunities to rationalise the e-comms landscape and set up robust information governance across e-comms and other 'surveillance' data.

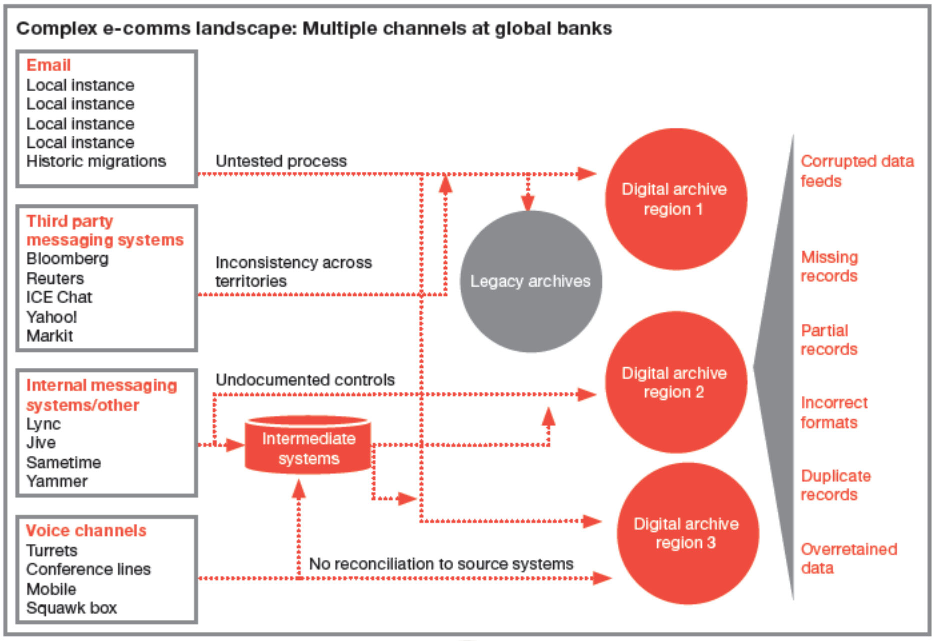
Regulatory pressure

Regulatory pressure: MiFID II 16(6/7)

Financial institutions must keep a record of all activities and transactions to enable regulators to fulfil their supervisory tasks.

The requirement includes all telephone conversations or electronic communications relating to client orders and dealing on own account.

Data must be retained for up to five years to support client requests, seven years for regulatory requests.



Cost and management pressure:

Limited management visibility of total user charges and licence costs for e-comms channels across the bank.

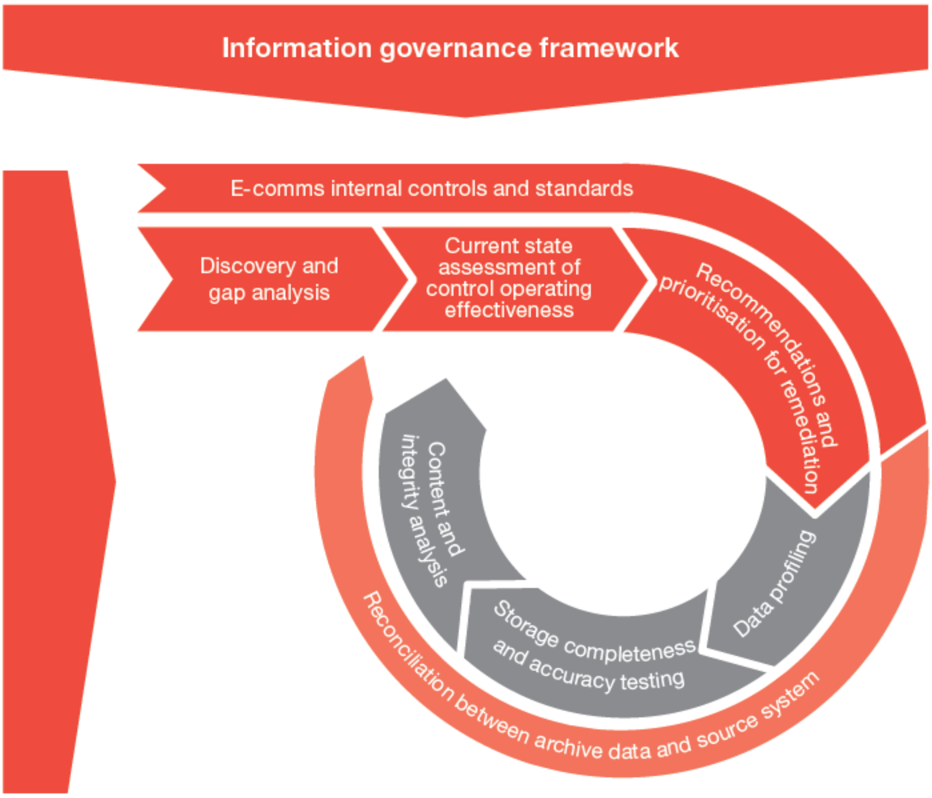
Limited management visibility of e-comms channel usage across the institution.

Potentially duplicate or superfluous e-comms channels in use.

Market pressure: Proliferation of new e-comms channels – Symphony launched March 2015 by 15 bank consortium.

Our approach

We can undertake an e-comms completeness and integrity review, which defines a target standard set of internal controls and tests existing controls against these. In parallel, we can test the data held in the digital archive to determine the extent of any data quality issues which require remediation. We can also apply our information governance framework to support you in determining data retention requirements and a defensible disposal framework for archived data.


Information governance framework
E-comms internal controls and standards
Discovery and gap analysis
Current state assessment of control operating effectiveness
Recommendations and prioritisation for remediation
Content and integrity analysis
Storage completeness and accuracy testing
Data profiling
Reconciliation between archive data and source system

Key deliverables

- E-comms internal control standard for the business.
- Information governance framework, and process for defensible data disposition.
- Detailed results from controls testing, and data completeness and integrity testing.
- Demonstrable evidence for the regulators showing the coverage and effectiveness of the controls in place to mitigate records management risks for Front Office messaging and voice recording.
- A remediation roadmap, with suggested priorities, to align with good practice and regulatory expectations.

Credentials

For a global bank we assessed the extent and effect of system/equipment failure on the quality of its retained communications data, and then provided the client with a method to measure the certainty of its disclosure to the regulator.

What PwC can offer you

Through the combination of our Information Governance practice, IT controls assurance and data analytics expertise, we are ideally placed to help review firms' e-comms controls and identify the extent of any data retentionáissues.

In addition we can help you develop your information governance framework.

Experience

We have expertise in assurance testing for IT systems, working with you to provide assurance around data integrity and supporting controls.

Expertise

We have a deep understanding of the key e-comms systems used by banks, and how communications records are used to support regulatory reviews.

Effectiveness

We have a proven track record in advising clients on the completeness and integrity of their communications data in order for them to comply with regulatory standards, requests and investigations.

Service

We work closely with you to learn about your business and requirements, to ensure that we provide a uniquely tailored service.

Leveraging our experience and expertise

Graham Ure

Partner
Surveillance data and technology

M: +44 (0)7889 644672
E: graham.ure@pwc.com

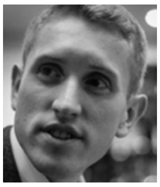
Rukshan Permal

Partner
Market abuse

M: +44 (0)7595 611533
E: rukshan.permal@pwc.com

Anne-Marie Edmonds

Director
Market abuse
M: +44 (0)7808 020659
E: anne-marie.edmonds@pwc.com



Alex West

Director
Market abuse
M: +44 (0)7841 567371
E: alex.e.west@pwc.com

Mark Chopping

Director
Surveillance data and technology
M: +44 (0)7889 645115
E: mark.chopping@pwc.com

pwc.com

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

190226-104028-GD-OS