OLIVER WYMAN

EMBARKING ON A JOURNEY FROM “SURVEILLANCE” TO “DETECTION”

AUTHORS
Chris DeBrusk, Partner
Allen Meyer, Partner
Adrian Murphy, Partner
Elena Belov, Partner

EXECUTIVE SUMMARY

Inappropriate conduct has cost the financial services industry a significant amount in direct losses, lawsuits, and fines since the last financial crisis. In response, banks have invested heavily in surveillance programs to identify employee misconduct manifesting via trading activity and electronic and voice communications. These programs are typically relatively simplistic and rules-based, and have often expanded over time to form a complex and inefficient web of firm-built and vendor solutions. While a radical transformation of existing surveillance programs would be quite difficult in the current environment, it is essential that financial institutions seriously consider and plan for what comes next, as it is clear that the status quo will not hold.

Many financial institutions face challenges across components of their capital markets-related surveillance frameworks, including current rules-based alert generation, lack of robust metrics, inefficient core processes, as well as sub-optimal underlying infrastructure. We recommend a strategic transition from the current rules-based approach towards a more dynamic, integrated, and conduct-oriented detection process. This strategy should be broader than selecting among new vendors, it should include investment in the human and technological capacity to enable financial institutions to more dynamically respond to emerging risks and more effectively and efficiently identify misconduct.

We recommend investment in two key capabilities to propel institutions towards this future state:

1. **Invest in an integrated data management environment:** invest in data sourcing and data management capabilities to ensure robust, accurate, and up-to-date information is continually available as the basis for analytics.

2. **Establish a Compliance Intelligence Unit:** set up a specialist team to analyze data for Compliance incidents and risks through both reactive and proactive means. The analysis performed by this team would be used to develop and update surveillance algorithms on a continual basis, and with a risk-oriented lens.

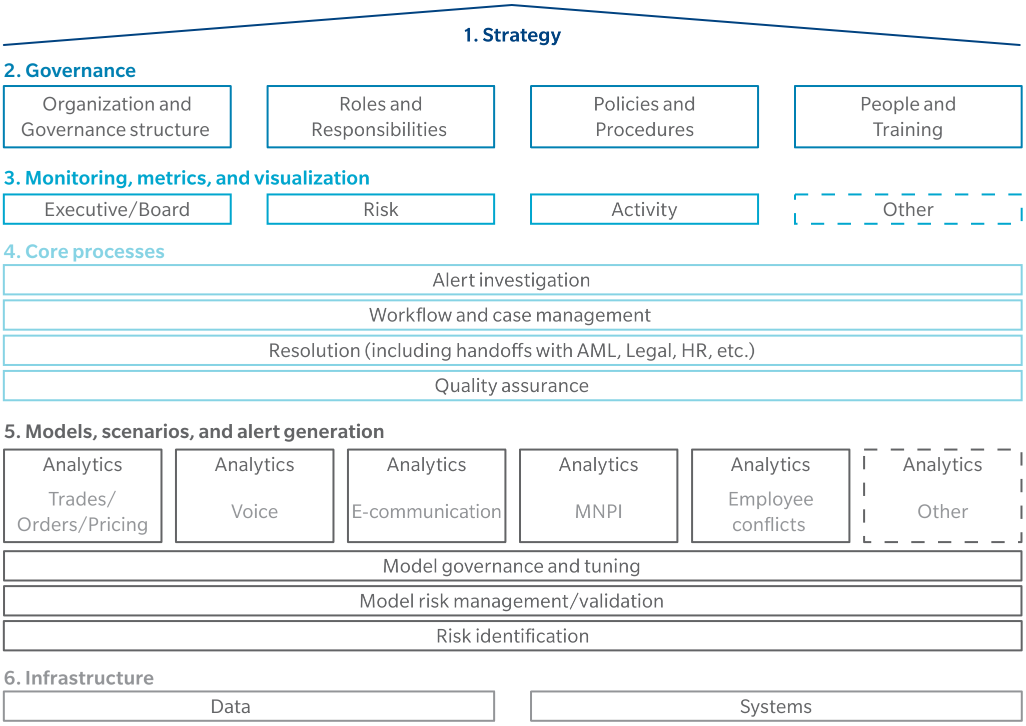
This journey will not be easy and will take thoughtful strategic planning and consideration of processes, data, analytics, technology and people. However, if institutions do not begin to plan and gradually implement a new surveillance strategy, they risk missing material misconduct and inefficiency, as well as regulatory criticism, fines and enforcement that will make a transition much more difficult to execute quickly in the future.

SHORTCOMINGS OF CURRENT STATE SURVEILLANCE FRAMEWORKS

Events over the last few years have highlighted serious misconduct across the financial industry, with numerous major banks named in investigations or lawsuits related to the FX and LIBOR scandals alone. Events such as these prompt reasonable questions from regulators, the public, and the institutions involved, as to why the misconduct was not detected internally by the first line of defense (the line of business) or the second line of defense (the Compliance function). These events ultimately resulted in billions of dollars of fines for the institutions involved, as well as significant reputational damage and remediation costs. In response, conduct expectations and regulatory requirements increased dramatically via bank specific remediation requirements and regulatory changes including the Market Abuse Regulation (MAR) and MiFiD II.

To holistically tackle this challenge, firms should consider how to initiate a transformation based on a strategic surveillance framework (see Exhibit 1), as the current state in most institutions is neither optimal nor sustainable. Many financial institutions have common shortcomings across a number of the framework's components and these shortcomings will need to be addressed to identify and prevent the types of misconduct that the industry has experienced in recent years, and new types that will originate in the future.

Exhibit 1: Typical surveillance framework components



1. Strategy

2. Governance

Organization and Governance structure	Roles and Responsibilities	Policies and Procedures	People and Training

3. Monitoring, metrics, and visualization

Executive/Board	Risk	Activity	Other

4. Core processes

Alert investigation

Workflow and case management

Resolution (including handoffs with AML, Legal, HR, etc.)

Quality assurance

5. Models, scenarios, and alert generation

Analytics Trades/ Orders/Pricing	Analytics Voice	Analytics E-communication	Analytics MNPI	Analytics Employee conflicts	Analytics Other

Model governance and tuning

Model risk management/validation

Risk identification

6. Infrastructure

Data	Systems

1. **Strategy:** Many institutions operate without a clear, top down vision or principles for their surveillance function. Surveillance strategies are typically responsive and remedial, designed to correct last year's problems rather than anticipate next year's. They also generally focus on satisfying regulatory and audit expectations, rather than being oriented towards detecting misconduct and protecting the bank.

2. **Governance:** Surveillance organizational structures are often arranged in silos that separate trade, e-communication, voice, insider trading and employee conflicts teams, leading to sub-optimal interaction between groups. This lack of collaboration makes it difficult to ensure that the dots are connected amongst groups. Surveillance teams can also have gaps in business knowledge and the technical skills necessary to detect and interpret sophisticated misconduct.

3. **Monitoring, metrics, and visualization:** The metrics used today to monitor surveillance activity and effectiveness typically do not properly support executive and Board level monitoring of risks in a way that is both holistic and digestible. Institutions could do more to better communicate surveillance activity and key risks to management. For example, creating a common dashboard that enables a timely view of emerging risks, surveillance accuracy and case management productivity.

4. **Core processes:** Case management is an area in which there is often underinvestment. Cases are addressed with limited prioritization, which results in the same resource allocation to case files regardless of associated regulatory or business risks. Additionally, while some efficiency and effectiveness metrics are being used for monitoring core processes, few financial institutions are regularly leveraging the results from previous cases to upgrade their alert generation rules or adjust case handling practices.

5. **Models, scenarios, and alert generation:** Existing surveillance models are often based on simple rules that do not leverage statistical methods or consider technological advancements which are becoming main-stream in other business areas (e.g. pattern analysis and vector analysis for text; sentiment analysis for voice; network analysis, etc.). Institutions will need to give deeper, more strategic thought to their existing risk identification processes to determine the actual problematic scenarios that ultimately should be fed into their models, rather than focusing on tweaks and upgrades to vendor default thresholds.

   Additionally, regulators are increasingly focused on the obligations of financial institutions to file suspicious activity reports (SARs) for a broad set of suspicious activities (e.g. market abuse, insider trading). To monitor this complex array of activity, institutions will need to ensure that surveillance models and model governance processes are robust. This will require significant improvement in the current quality of data preparation, the explanation of logic underpinning the model and the supporting documentation.

6. **Infrastructure:** At the foundation of any surveillance framework are the data and systems capabilities which support all analyses and processes. Unfortunately, data is rarely integrated across different sources (e.g. trades, physical activities of employees, voice communication, e-mail communication, etc.). This negatively impacts the ability of the firm to detect events that are made up of multiple activities which are collectively suspicious. Additionally, data is often of poor quality in terms of accuracy and completeness which often results in the generation of excessive false positives.

DEEP DIVE: WE BELIEVE THAT IMPROVING ALERT GENERATION HAS THE POTENTIAL TO DRIVE THE MOST SUBSTANTIAL GAINS ACROSS THE WHOLE FRAMEWORK

Despite the shortcomings of existing Compliance surveillance programs, a complete dismantling of the current state is not required to begin upgrading to a more strategic program, nor is it practical given the current environment. By focusing on incrementally improving alert generation, institutions can start the transition to a more flexible forward-looking surveillance approach by building on the foundation of their existing infrastructure.

1. VENDOR ALERT GENERATION

To generate surveillance alerts, most financial institutions currently rely on vendor solutions, which utilize basic heuristics or rules-based approaches to select risk factors and set thresholds, rather than actual customer or employee behavior. These rules rarely leverage the full array of knowledge and data available within a financial institution. The limited sophistication of these platforms causes a high volume of alerts, many of which are false positives, which in turn result in a corresponding poor hit rate and a high level of effort performing manual downstream review and investigation activities.

While many firms derive comfort from having common, well known vendor packages forming the basis for their surveillance infrastructure, the approach of subjective threshold setting that is the norm with nearly every vendor is becoming more difficult to defend. Additionally, updates to these threshold based scenario packages are dependent on coordination between vendors and internal IT, which often results in changes to address emerging risks being slow and expensive. Ultimately, the limited ability for individual institutions to customize scenarios to meet their specific requirements means they end up casting a wider and less effective net when identifying suspicious activity.

2. TRADITIONAL ALERT GENERATION WITH ANALYTICS LAYER

To address these issues, some financial institutions have started to introduce hybrid approaches that combine existing vendor solutions with an in-house developed analytics layer to further filter and prioritize alerts. The advantage of this type of approach is that it leverages existing vendor packages and set-up, while beginning to move towards a more customized solution. This bespoke analytics layer can become the first step in development of a target state alert generation framework.

3. INTEGRATED AND CUSTOMIZED ALERT GENERATION

Advanced financial institutions are starting to think about creating customized behavior and risk-based alert generation systems. We expect that in the future, such solutions will be flexible and adaptive, they will leverage a wide range of available data, and will be continuously updated to account for emerging risks – thus ultimately reducing false positives and allowing suspicious behavior to be more easily identified.

Exhibit 2: Expected evolution of alert generation practices

1. Traditional solution Vendor alert generation	*Vendor systems used to generate alerts that are sent to analysts for review*	+ Regulators often have familiarity with common vendor packages + Huge upfront investment so great reluctance to move from this approach – Rigid, slow and expensive for updating alert-generating scenarios – Basic logic can result in high volume of false positives
2. Traditional solution with analytics Vendor alert generation with analytics layer	*Vendor systems used to generate surveillance alerts with further analytics added to prioritize alerts for case management*	+ Alerts are prioritized for case management resources + Minimal dislocation of vendor-based framework – Lack of complete flexibility and agility – Limited ability to adapt or to proactively identify issues
3. Behavior- and risk-based solution Integrated and customized alert generation	*Platform derived from sophisticated analytics; alerts customized to institutional risks, continuously iterated, and forward-looking*	+ Minimum false positives generated + Continuous process improvement + Flexible and adaptive systems + Integration of previously siloed solutions – Investment, time, and expertise required to setup

TO ACHIEVE THE BEHAVIOR – AND RISK BASED SOLUTION, WE RECOMMEND INVESTMENT IN TWO KEY CAPABILITIES TO PROPEL INSTITUTIONS TOWARDS DETECTION OF BAD BEHAVIOR

1. INVEST IN AN INTEGRATED DATA MANAGEMENT ENVIRONMENT

To transition to a more strategic surveillance implementation, financial institutions will need to invest in data sourcing and data management capabilities to ensure robust, accurate, and up-to-date information is continually available as the basis for performing analytics.

DEFINING A BUSINESS LEVEL DATA DOMAIN MODEL

A key first step to defining a comprehensive surveillance data environment is the definition of a business level domain model to fully map each type of data that is consumed for surveillance activities, and the key relationships between different types of data. Once defined, this model can be used to drive all data sourcing efforts, including both structured and semi-structured information and ultimately become the basis for data quality metrics. At its most comprehensive state, it should include order and transaction details, money movement, associated P&L, electronic and voice communication and supporting information like building access and market events.

CONTRACTS BETWEEN SURVEILLANCE AND SOURCES OF DATA

Comprehensive data sourcing requires an approach based on the definition and implementation of "contracts" between the surveillance function and sources of data. Each contract should clearly state the type of information being exchanged, the expected level of quality and completeness, timing and any other considerations required to define the service level agreement (SLA) criteria that will ensure that both the provider of the information, and the consumer of the information (surveillance) can meet the other's expectations.

DEDICATED DATA TEAM

A data team that is dedicated to the surveillance function (or ideally the entire Compliance department) should be established to manage data and serve as the "go-to people" for data information requests and can ensure there is a robust understanding of all source systems within the surveillance function and strong relationships with frontline and other system owners. The responsibilities of this team can include maintaining the documentation of data models, defining data quality metrics, acting on data quality exception reports and discrepancies, executing new data sourcing projects, and maintaining a knowledge base of data problems and solutions.

A dedicated data team, once deployed can significantly impact the productivity and effectiveness of the overall surveillance function. The work they do is critical for enabling a move to more a comprehensive analysis framework that is not frozen in silos and leverages the entirety of the data available across the financial institution.

2. ESTABLISH A COMPLIANCE INTELLIGENCE UNIT (CIU)

Some leading financial institutions are already investing in data analysts and sophisticated technology toolkits which are critical ingredients for a more dynamic and effective surveillance program in the future. More specifically, we believe that financial institutions would be well served to establish a Compliance Intelligence Unit (CIU) – A team whose purpose is to analyze data for Compliance incidents and risks through both reactive (e.g. investigations) and proactive (e.g. war gaming, pattern identification) means. The analysis performed by these teams would then be used to develop and update surveillance algorithms on a continual basis, and with a risk-oriented lens.

CIU COMPOSITION

Members of a CIU will bring to the role a wide range of skills, including regulatory, business, investigative and data analysis expertise, along with specialist skills. Members can come from a wide range of career backgrounds, including former traders, data scientists, and quantitative analysts. By creating a team that is cross functional, financial institutions can ensure that they bring a comprehensive perspective on the multivariate nature of misconduct; one that is data-driven, self-improving, and forward-looking.

TECHNOLOGY TOOLKITS

To be effective, CIUs need to be equipped with the appropriate technology toolkits that span data management, transformation and analytics platforms. Infrastructure that is able to ingest and manage massive data sets is critical to allowing the CIU to expand its analytics work outside of the traditional trade, position and reference data spaces and gain access to a wide range of data types and large amounts of historical information and associated ID/temporal reference points. Sophisticated, analyst accessible data transformation tools will allow members of the CIU to reconfigure data in nearly endless ways, creating new relationships, applying filters and enhancing data streams with supplemental information. Finally, the toolkit will need to provide for flexible reporting and visualization of both raw data and the results of analytics, either in an ad hoc way or via standard dashboards. In the future, the CIU will need to be able to deploy advanced technology such as machine learning to test advanced surveillance concepts and monitor risks that are not contemplated in today’s environment.

SOPHISTICATED ANALYSIS

Given access to integrated data and technology toolkits as described above, these units can help hone in on misconduct more effectively during investigations, as well as predict it in the future. When an alert is triggered, an investigation can probe not only the actions that resulted in the alert (e.g. trading behavior), but also supplemental variables that will provide further insight into whether, and to what extent, bad behavior exists. Network diagrams can visually connect voice communications, employee information, and trading behavior to create a map of interactions and behaviors which is more complete than any univariate alert.

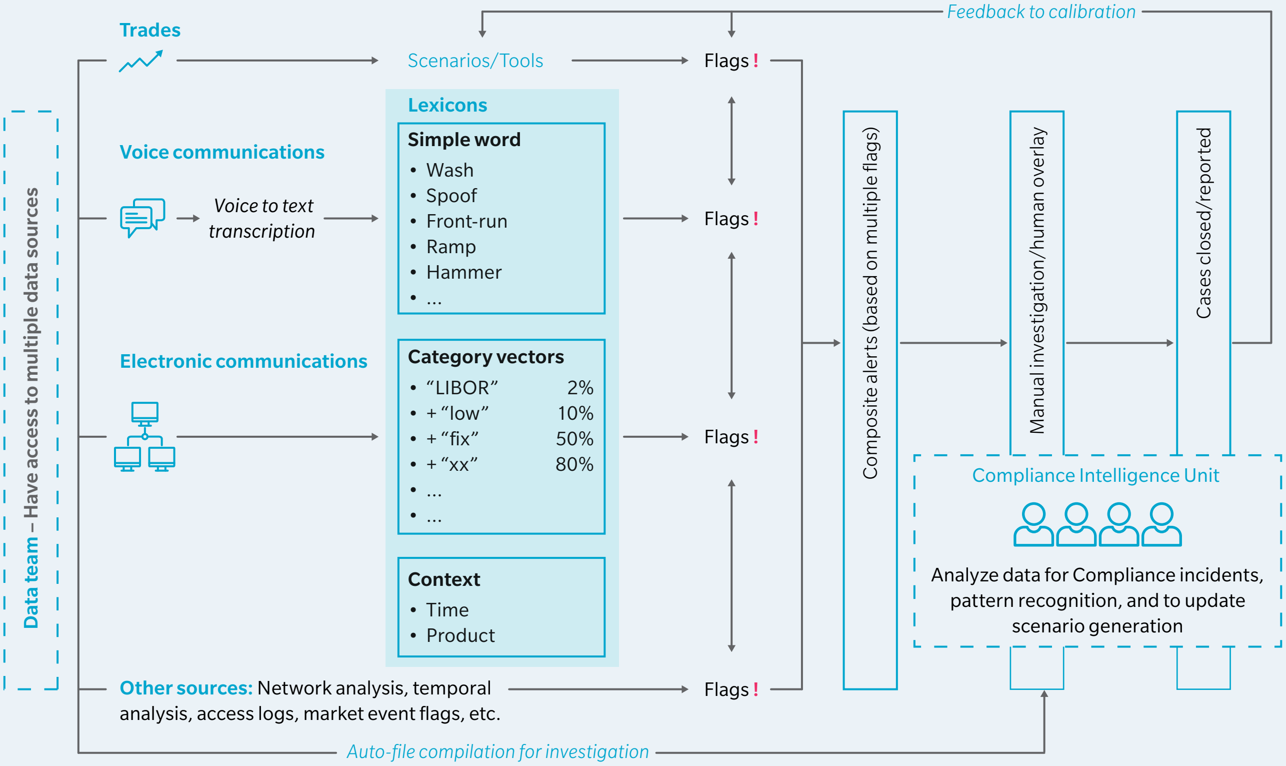
CIUs can also drive “what-if” analysis, or war gaming, in which they theorize about risks that may not yet be covered by existing metrics and analysis. They can ask questions like “We have observed this type of abuse in isolated cases, but what if it is more widespread?” or “My peer firm has experienced a certain type of misconduct, am I at risk for the same type?” We have received multiple regulatory data requests on this, what is it that they might be looking for?” The flexibility inherent in the infrastructure supporting the CIU will permit bespoke analysis tailored to these questions. The team can conduct deep-dives or follow leads uncovered by the analysis without limitations imposed by lack of technical proficiency, data availability, or vendor inflexibility.

THE TARGET STATE WILL INVOLVE MORE CUSTOMIZATION, ITERATIVE FEEDBACK, AND FORWARD-LOOKING ANALYSIS

An example target state model for surveillance is illustrated in Exhibit 3. We expect the solution of the future to include the following key capabilities:

- **Integration solution across data channels:** Composite alerts, based on multiple flags will be generated by leveraging a wide range of information sources including trade data, voice communications, e-communications, and other data.
- **Proactive analysis (e.g. pattern recognition):** Financial institutions will develop next generation models and scenarios, based on extended data sources to identify new patterns of behavior that could signal suspicious activity rather than reacting to potential breaches based on simple thresholds. One emerging area of surveillance is the monitoring of person-to-person networks (i.e. who is communicating with who) which has been shown to have high predictive potential. Ultimately, the combination of new innovative techniques with access to real-time data will identify breaches as they occur, or even prevent them altogether.
- **Forward-looking scenario analysis (e.g. war-gaming):** As referenced previously, the CIU will incorporate expert-driven war gaming or scenario analysis workshops into their processes. The intent of this approach will be to identify emerging Compliance risks that have not been experienced historically or reading across from one business to another, and to develop additional, supplementary alerts.

Exhibit 3: Illustrative view of target state for surveillance



Feedback to calibration
Trades
Scenarios/Tools
Flags !
Data team – Have access to multiple data sources
Voice communications
Voice to text transcription
Lexicons
Simple word
• Wash
• Spoof
• Front-run
• Ramp
• Hammer
• ...
Flags !
Electronic communications
Category vectors
• "LIBOR" 2%
• + "low" 10%
• + "fix" 50%
• + "xx" 80%
• ...
• ...
Flags !
Context
• Time
• Product
Other sources: Network analysis, temporal analysis, access logs, market event flags, etc.
Flags !
Composite alerts (based on multiple flags)
Manual investigation/human overlay
Cases closed/reported
Compliance Intelligence Unit
Analyze data for Compliance incidents, pattern recognition, and to update scenario generation
Auto-file compilation for investigation

CONCLUSION

Few financial institutions have moved towards a surveillance strategy that focuses on predicting and proactively addressing the areas of greatest risk. As technology moves quickly forward and many financial institutions emerge from a period of intense remediation activity in their surveillance functions, they are presented with great opportunities to revisit surveillance strategy. This strategy should be broader than selecting among new vendors and should include investment in the human and technological capacity to enable financial institutions to more dynamically respond to emerging risks and more effectively and efficiently identify misconduct. In doing so, Compliance functions should launch a data initiative, or make sure data experts have a significant role in programs of this nature, because robust data, consistent data management and internal data expertise are essential pre-conditions to leaping forward with the surveillance program. Similarly, setting up a small team now with the right combination of skillsets alongside the existing surveillance teams to begin to more proactively address emerging risks through the use of emerging technologies will help seed the transformation that we think is necessary to truly move from “surveillance” to “detection.”

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS

+1 212 541 8100

EMEA

+44 20 7333 8333

ASIA PACIFIC

+65 6510 9700

ABOUT THE AUTHORS

Chris DeBrusk, Partner
chris.debrusk@oliverwyman.com

Allen Meyer, Partner
allen.meyer@oliverwyman.com

Adrian Murphy, Partner
adrian.murphy@oliverwyman.com

Elena Belov, Partner
elena.belov@oliverwyman.com

EMEA CONTACTS

Serge Gwynne, Partner
serge.gwynne@oliverwyman.com

Jennifer Tsim, Principal
jennifer.tsim@oliverwyman.com

CONTRIBUTORS

Jerry Wu, Associate
Diane Shahan, Senior Consultant

APR CONTACTS

Wei Ying Cheah, Principal
weiying.cheah@oliverwyman.com

Jayant Raman, Prinicpal
jayant.raman@oliverwyman.com

www.oliverwyman.com

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.

OLIVER WYMAN