Getting Surveillance Right:
Protecting Banks’ Reputation and Profitability

High performance. Delivered.

BIG PICTURE

REPUTATION

PROFITABILITY
Banks have spent vast amounts on initiatives related to regulatory compliance since 2008, but major events continue to affect banks’ reputation and profitability. Banks paid over $3.7 billion in fines in 2012 and 2013 for attempts to fix the London Interbank Offered Rates (LIBOR), and individual banks have paid multi-million and sometimes multi-billion dollar fines related to offenses ranging from insider dealing to benchmark rates fixing to rogue trading.

In most if not all cases, proper surveillance and early notification of improper and/or illegal activities could either have prevented the events from taking place or could have greatly limited their scope and the amount of damage inflicted. By not investing in surveillance capabilities – and by failing to coordinate and integrate such capabilities – banks risk severe regulatory and reputational damage. Capital expenditures that might otherwise be earmarked for growth and expansion of core businesses are diverted to cover legal costs, fines, operational fixes and reputational repairs.

There are other, more lasting costs related to poor surveillance. In our view, current and potential customers are far more likely to work with firms whose focus is on their own day-to-day business rather than those who have breached regulations and damaged their reputations.
The Future of Surveillance

New and more innovative approaches to surveillance will be dictated not so much by banks' expenditures on people, process and technology as by their approach to the entire concept of surveillance. At present, surveillance is an activity that is driven primarily by regulation (although there is a competitive advantage derived from being best-in-class). The data generated by surveillance activities is typically confined within specific business units or trading desks, available only on a "need to know" basis.

Surveillance is often designed to identify specific actions taken by individuals within the organization. The thresholds for flagging such actions tend to be similar for all groups and business areas, based on an analysis of structured data using clearly defined algorithms.

As banks' recent experience indicates, this overall approach leaves significant coverage gaps. Forward thinking banks are moving toward a surveillance model which is driven by organizational culture rather than specific regulations. In this model, data is available as needed, not kept in silos, supporting surveillance that takes place in real time and is proactive, rather than reactive. Having access to front to back data and relevant controls can help ensure that breaches are detected early or are completely avoided. Take an example of a wealth manager trading on behalf of a client. Data from pre-trade onboarding activities (Anti-Money Laundering/Know Your Client/Investment Profile) can be overlaid to completed trades to help identify potential suitability or market abuse patterns. Historic associations alongside current transactions can provide additional information to the bank which was previously not available.

Another characteristic of the future state of surveillance is the use of analytics to identify patterns of activities and behaviors, rather than specific events that cross predetermined thresholds. The thresholds used are flexible, based on profiles that reflect not just individual behavior but the normal activities of an entire trading desk or business unit. Finally, new model surveillance employs analytics using not just structured data – such as that generated by trading activity – but also unstructured data generated by emails, social media, and even telephone conversations. There is also the opportunity to overlay this data with HR and individual employee compliance data to look for patterns and potential triggers that could lead to a breach.
The Big Picture: Preventing Problems Before They Occur

Banks engage in a number of different types of surveillance, including trade surveillance and communications surveillance. Banks set trade limits and review breaches of such limits as they occur. In addition, profit and loss reviews and other control functions, as well as other compliance, back office and middle office reconciliation activities, help prevent abusive or illegal conduct.

Currently, however, these surveillance functions are rarely aggregated; in other words, surveillance is conducted desk by desk or business by business. Data gathered by one surveillance team is not shared with other teams, even though such sharing can provide both preventative and post-event investigative capabilities that can help mitigate risk. These separate surveillance functions include:

- **Financial Industry Regulatory Authority (FINRA)** – monitoring brokers for overcharging customers, making unsuitable investments and other infractions;
- **Social media** – tracking employees’ use of social media, both inside and, in some cases, outside the organization;
- **Market** – monitoring trading and trading functions to prevent illicit trading activities;
- **Employee** – monitoring employee email, personal trades and, in certain cases, phone calls;
- **Financial crime** – Anti-Money Laundering (AML), Anti-Bribery and Corruption and actions in contravention of sanctions.

As currently structured, surveillance is a reactive process using tools that look at past patterns to determine if a breach has occurred. For surveillance to realize its full potential, it should become more proactive. We believe that a planned, systematic approach to investing in surveillance capabilities could generate significant returns, not only in terms of preventing and minimizing adverse events, but in demonstrating banks’ commitment to being a stable, dependable business partner.

Firms should consider using advanced data analytics – harvesting information from new channels such as social media – to create predictive analytics. Through focused training and faster response, firms could help prevent breaches in areas identified as having a high potential for undesirable activity. Ideally, banks should be able to turn post-event investigative data and tools into preventative detection systems that utilize analytics and real-time reporting to spot deviations from behavioral norms as they occur. Using these methods, banks could also help create increasingly sophisticated risk profiles as they attempt to pre-empt breaches.

In our experience, the total cost of investing time and resources in comprehensive, preventive surveillance is often less than the cost of investing in disconnected, group-by-group efforts – and the results are better. The total amount invested can be spread over time, with priorities aimed at targeting gaps and weak points to provide immediate returns.

For the “Big Picture” approach to be effective, however, banks are encouraged to synchronize data across functions, allowing for pattern recognition and analysis from group to group. For example, a breach in value-at-risk (VAR) limits set by the market risk function – accompanied by increased trading activity and re-booked trades seen in the Profit and Loss (PnL) Explained – could be linked together by compliance functions following flagged counterparties. This, in turn, could lead both to preventive measures and to actions taken to address the unauthorized activities, rather than being used as investigative tools once the damage has been inflicted.

In addition to data synchronization, big picture surveillance requires advanced analytics and data technologies to run increasingly sophisticated queries across ever-larger data sets. Firms will need to invest in updating and maintaining their technical abilities.

As seen in Figure 1 below, the surveillance function encompasses banks’ entire risk framework and affects many areas of concern. Enhanced surveillance capabilities can improve banks’ overall operational, regulatory and reputational risk management programs.

**Figure 1. Impact of Surveillance Function on Risk Management**

Source: Accenture, January 2015
Bringing Business Units Together

To obtain a surveillance picture that is not only “big” but also comprehensive, different business units and functions need to create a pool of data that is regularly monitored and analyzed to identify patterns and anomalies. Traditionally, the business units that control and monitor activities within banks sit in different areas, with different objectives and reporting lines. Teams within compliance, risk, client onboarding, HR, product control and the operations have varied control functions and verify different aspects of trades and transactions. Identifying relevant data and sharing it within a cross-functional surveillance unit can help build patterns and identify both current and potential wrongdoers.

For proper execution, these teams and functions should provide input to a centralized location, with the compliance function serving as the overall surveillance owner.

Compliance
- Trade Surveillance (Looking at market abuse instances and patterns)
- Communication Surveillance (Looking at communications and behaviors)
- Control Room Surveillance (Surveillance of information abuse/conflicts of interests)
- Regulatory Risk Review (Review of desk trading behaviors, authorizations and regulatory gaps)
- Financial Crime (Assessing trade counterparty eligibility, frauds and crimes)

Risk
- Trading Desk – Market Risk Management (Looking at traders/desks market risk profiles to identify aberrations on granular and consolidated levels)

Product Control
- Profit and Loss Monitoring (Profit and Loss allocations, patterns and explanations)
- Trader Surveillance (Managing chinese walls, trader mandates, traded product assessments)

HR
- Leave Patterns/Block Leaves (Patterns of employees’ leave behaviors)
- Employee Onboarding (Understanding potential employee’s background)

Client Onboarding
- AML (Understanding how and where the client money is allocated)
- Know Your Client (Understanding client’s business, history and associations)
- Business Objectives (Understanding client’s expectations concerning the bank)

Current Solutions
Most currently available surveillance solutions are unilateral offerings; focused on surveillance of one particular area. In many cases, the same vendor offers different solutions for different surveillance requirements.

While this works well at one level – when the product differentiation is clear – unilateral offerings do not provide optimal opportunities for collaboration, data sharing and pattern identification. In addition, unilateral offerings focus on specific types of information such as unstructured data, structured data, exchange activities, and unauthorized trading. Vendors are taking advantage of advances in big data, analytics and unstructured data analytics, but true cross-functional offerings are not yet available.

Implementing a Process-Driven Solution
We have identified three key elements that in our view are essential for a favorable transformation to a competent, proactive big picture surveillance function:

1. A commitment from top management expressed clearly as a set of working principles for team leaders and members;
2. Measured and focused investment in the right technology and tools;
3. The right culture, developed and fostered throughout the organization. This means that top management of each business unit and function should understand the benefits of actively sharing data.

The basic steps toward an effective, integrated surveillance framework include:

1. Creating an accountable risk governance structure for surveillance activities – with an executive committee representing members of involved business units – responsible for reviewing highest priority issues and supervising ongoing surveillance improvement.
2. Enhancing preventive risk identification methods.
3. Defining relevant data collection and data sharing requirements for different teams.
4. Integrating data across functions for a more comprehensive view and more effective, aggregated risk analysis.
5. Creating a centralized tracking and reporting center of excellence, using industry leading practices, technology, and coordination across functions.
6. Creating normal profiles of different trading businesses, trading desks and individual traders based on historical analysis.
7. Studying deviations, alerts and issues related to these normal profiles.
8. Reporting relevant findings to the appropriate stakeholders.
Maturity Model for Surveillance

It has been our experience that the adoption and implementation of big picture surveillance is a multi-tiered process. Acceptance and implementation will vary from bank to bank but typically takes place in three phases.

In Phase One, banks address their immediate needs, identify teams and define their requirements, with a focus on "at risk" areas and enhanced preventive capabilities. This phase usually includes a current state assessment of surveillance capabilities, followed by a budget and plan for execution based on the assessment’s findings and recommendations. Key tasks include aligning the management team, identifying stakeholders, defining the right data and how to share it. The risks to be mitigated and the criteria for success are agreed upon, as well. During this phase, banks also define an effective governance organization to help manage and implement the plan.

In Phase Two, the banks define what “normal” activity is and then begin to define requirements for the desired target state for surveillance. Teams review analytics and other technology solutions and define the process, needed resources and training to help reach this state. Data is integrated from source systems and core functions within a business area and may be re-aligned; for example, compliance control and surveillance teams may take responsibility for trade surveillance activities. Phase Two also includes the first steps in a phased implementation approach toward the target state, such as deployment of trader and client profiling technology, behavioral mapping and other innovations.

In Phase Three, big picture surveillance capabilities are in place and have begun to identify gaps and anomalies. The surveillance management structure is in place and the organization may have adapted a center of excellence model. External data from social media, newswires and elsewhere may be integrated into surveillance models. Training materials are developed and refined, and the entire process is updated as needed. Phase Three is marked by an emphasis on culture and human resources, as these are essential to the success of the ongoing program.

Benefits of Seeing the Big Picture

In our view, banks committed to improving surveillance through an integrated, big picture approach should see quantitative improvements in a number of key metrics:

- More breaches detected, with a reduced number of false positives;
- Lower costs associated with each incident;
- Faster detection leading to fewer incidents escalating;
- Over time, a reduction in breaches as employees, counterparties and others realize the extent of the bank’s surveillance capabilities.

While effective surveillance requires investment in technology and human resources, the returns in terms of risk mitigation and enhanced reputation can be significant. Banks should look at their current “need to know” surveillance practices with these potential benefits in mind.
About the Authors

Samantha Regan is a managing director in Accenture's Finance & Risk Services. She has 17 years of global experience in banking and capital markets gained within industry and consulting. Samantha specializes in regulation and compliance and has been deeply involved in developing Accenture’s regulatory and compliance management capabilities. She is the Global Regulatory & Compliance lead for Accenture’s Finance & Risk Services practice.

Chris Beck is a manager, Accenture Finance & Risk Services, based in Chicago. Specialized in strategy planning, operational risk management and compliance risk management, Chris brings his solid experience and skills in these areas to help financial institutions define and implement their governance and risk management structures.

Amit Khare is a manager, Accenture Finance & Risk Services. He is a CFA with over 9 years of global experience in capital markets working across multiple asset classes in sales, trading, risk and compliance functions. Amit specializes in the definition and implementation of surveillance and control functions, focused on complex products in the investment banking space.

Notes


About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with approximately 319,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world’s most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.

Disclaimer

This document is intended for general informational purposes only and does not take into account the reader’s specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.