Research partner

EY
Building a better working world

Independent research by

Chartis

The Future of Trader Surveillance

The ABCD of Successful Surveillance

October 2017

About Chartis

Chartis Research is the leading provider of research and analysis on the global market for risk technology. It is part of Infopro Digital, which owns market-leading brands such as Risk and Waters Technology. Chartis's goal is to support enterprises as they drive business performance through improved risk management, corporate governance and compliance and to help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on virtually all aspects of risk technology. Areas of expertise include:

- Credit risk
- Operational risk and governance, risk and compliance (GRC)
- Market risk
- Asset and liability management (ALM) and liquidity risk
- Energy and commodity trading risk
- Financial crime including trader surveillance, anti-fraud and anti-money laundering
- Cyber risk management
- Insurance risk
- Regulatory requirements including Basel 2 and 3, Dodd-Frank, MiFID II and Solvency II

Chartis is solely focused on risk and compliance technology, which gives it a significant advantage over generic market analysts.

The firm has brought together a leading team of analysts and advisors from the risk management and financial services industries. This team has hands-on experience of implementing and developing risk management systems and programs for Fortune 500 companies and leading consulting houses.

Visit ***www.chartis-research.com*** for more information.

Join our global online community at ***www.risktech-forum.com***.

About EY

EY is a global leader in assurance, tax, transaction and advisory services. Our professionals are dedicated to helping our clients transform their businesses and pursue the greatest opportunities for growth. We assemble the right team, drawing on our global network of professionals to help clients address business, regulatory and technology-focused challenges.

Collaboration is at the very heart of what we do at EY, and our dedicated global technology and innovation networks help us provide clients with market-leading and insightful perspectives. EY assists the world's leading banks in defining the right approach to harness disruptive technologies to better enable, enhance and transform their business, and in turn to better serve their clients.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ***ey.com***.

The better the question. The better the answer. The better the world works.

About the EY contributor

Glenn Perachio

Glenn is a Partner in Ernst & Young (UK) LLP's Forensic Technology and Discovery Services group. He leads EY's Assurance Managed Services UK team, working with clients in the areas of Forensic Data Analytics, Monitoring and Supervision, eDiscovery, IT Forensics, Information Governance, and Legal Information Technology. Glenn is also EY's Financial Crime Market Abuse and Trader Surveillance Solution Leader.

Glenn has over 25 years' experience in the field, and has worked with clients on some of the largest litigation and regulatory matters in the tobacco, oil and gas, and financial services sectors. Recently his work in financial services has focused on market abuse cases in LIBOR and FX benchmarks. He has helped clients navigate data and risk challenges through the lifecycle of investigations, to remediation, to prevent and detect strategies and solutions for e-communications and trade data monitoring, employing techniques such as robotics and artificial intelligence. For European banks he has advised and tested data analytics methodologies to identify issues and improve screening accuracy and alert management in relation to AML remediation.

Glenn has chaired panels and hosted roundtables at legal and regulatory events across the globe, including LegalTech, The Lawyer Legal CIO Forum, IQPC Information Governance and eDiscovery events, The Economist CIO roundtables, and the UK's eDisclosure Information Project.

Additional insights were provided by EY's Natalie Rapalo (Financial Services – Fraud Investigation & Dispute Services) and Tom Goodman (Financial Crime Analytics).

Table of contents

List of figures and tables

1. Executive summary

Spelling it out

Market abuse is a growing concern for financial institutions (FIs). A number of high-profile events (the LIBOR and Foreign Exchange [FX] trading scandals, for example, as well as those connected with the manipulation of ISDAFIX earlier this year) have resulted in hefty fines for FIs – more than $19 billion for LIBOR and FX alone[1] – pushing trader surveillance up the agenda.

Trader surveillance is complex, however, and objective truth is hard to come by. The role of traders is to make money for their firms, and in practice the line between good behavior and abuse can sometimes be blurred. The process presents several challenges, such as extracting clear signals from the 'noise' of the markets, and providing evidence of intent and market abuse without lengthy recourse to diverse sources of information. To make matters worse, among these sources is communications data, which is traditionally not well-integrated with trade monitoring systems.

To fully address the challenges they face around trader surveillance, FIs must leverage four success factors, which we have labeled 'the ABCD of successful surveillance':

A

Accuracy…
More advanced and effective analytics – including integrated monitoring of communications and trading activity – to deliver better quality alerts across data types, asset classes and trades.

B

Breadth…
More effective and flexible workflow engines, and robotic process automation (RPA), to draw more information from a wider array of trading venues and asset classes. This can reduce the workload involved in investigating alerts, and help FIs develop systems with improved drill-down capabilities, as well as the ability to analyze metadata.

C

Culture…
Trader surveillance systems that work within a robust governance framework and the three lines of defense. These can reinforce a culture of compliance by delivering quantifiable information about front-office traders' behavior within a conduct risk framework.

D

Data…
Integration, validation, cleansing and standardization, to ensure that the data FIs feed into their systems is accurate, and can be audited and validated across a variety of sources.

Change in the air

The need for effective trader surveillance systems is becoming more pressing. So far, the default position for FIs has been to use systems designed primarily to meet the requirements of regulators. While regulations allow for a certain degree of flexibility when addressing trader surveillance, FIs are wary of distinguishing themselves too much from their peers – there is safety in being part of a group of institutions that all manage risk in the same way. As a result, there has been only modest technical advancement in this space.

[1] ***http://www.bankofengland.co.uk/markets/Documents/femrjun15.pdf***

Yet this picture is changing rapidly. Increasingly, rather than matching their trader surveillance capabilities to those of the bodies that regulate them, or even their peers, FIs are looking to establish their own leading practices. But why? And why now?

The key drivers of change are:

- **Regulators' desire for more 'semantic' information around trades**[2]. This has been driven largely by the Market Abuse Regulation (MAR). But it is emerging as good market practice, driving a more holistic approach to surveillance that encompasses electronic communications (e-comms) and trade monitoring.

- At the same time, regulators and market drivers are pushing **many FIs to expand the remit of their surveillance to cover a broader range of asset classes**, such as fixed-income, commodities, and other Over-the-Counter (OTC) products. Meanwhile, new trading venues such as Organized Trading Facilities (OTFs) must be catered for. Across these new assets and venues, systems originally designed for more traditional, 'regulated' asset classes (such as equities) are struggling under the weight of an increasing number of trades, idiosyncratic reporting requirements, and the sheer volume, variety and velocity of the data involved.

- **Trader surveillance systems are also generating thousands of alerts per day**, more than FIs' compliance teams can feasibly monitor. This is pushing up costs, as FIs expand their compliance departments with additional Full-Time Employees (FTEs) to keep pace. Not surprisingly, FIs want to increase the quality of their alerts, and speed up how they process them.

In a recent Chartis survey[3], 71% of respondents claimed to be in the process of upgrading their trader surveillance systems. Crucially, financial resources do not seem to be a big concern in these projects: only 5% of respondents named budget availability as their biggest challenge. Global expenditure on trader surveillance is also increasing: analysis by Chartis points to a rise in spend of 5% this year, taking it to $758 million by the end of 2017.

Clearly then, FIs understand the need to improve their trader surveillance, and have allocated resources to meet it. Effective surveillance can be a vital tool in an FI's fight against market abuse, and help to reduce workloads and boost efficiency. But in the drive to establish best-in-class trader surveillance, FIs are repurposing their existing systems, which are struggling under the strain. Nevertheless, by following the steps outlined here, FIs can achieve broader, more accurate surveillance, using the best, most relevant data, and framed within the right organizational culture.

[2] *The Market Abuse Regulation (MAR) and the Regulation on wholesale Energy Market Integrity and Transparency (REMIT), for example, require alerts of market abuse to identify 'intent'.*
[3] *For more details, and a breakdown of respondents, see Appendix A.*

2. Background and context

Defining trader surveillance

For the purposes of this report we have defined the process of trader surveillance as *investigating an organization's activities for indications of market abuse*. This includes:

- Detecting market manipulation, insider dealing and misuse or disclosure of Material Non-Public Information (MNPI).
- Monitoring and analyzing trading and market activity and other relevant data, such as e-comms, voice and Profit and Loss (P&L) information.

The trader surveillance process has five steps (see Figure 1):

- Each relevant data source is surveilled.
- Alerts are generated according to potential types of abuse.
- Possible market abuse scenarios are reconstructed.
- Actions (escalation or reconciliation) are taken.
- Results are documented, reported and archived.

In practice this means monitoring data such as trades, orders, instructions to trade and communications across a variety of asset classes, product types and markets.

Figure 1: The trader surveillance process

Source: Chartis Research

This complex, multi-factor process also often overlaps with other areas of risk management, including:

- Unauthorized/rogue trade monitoring.
- Front- and middle-office tools, including operational risk management, Governance, Risk and Compliance (GRC) platforms and IT surveillance.
- Best-execution compliance (i.e. ensuring that firms are doing enough to obtain the best possible results for their customers, by taking into account factors such as price and cost under regulatory constraints).
- The broader compliance agenda for financial crime (including Anti-Money Laundering [AML], sanctions, Know Your Customer [KYC] and fraud).

What's driving trader surveillance?

Historically, sell-side firms have focused on trader surveillance, but regulations such as Markets in Financial Instruments Directive II (MiFID II) and MAR are increasing surveillance requirements for the buy-side and trading venues, and moving them into areas such as energy and commodities markets[4]. And for buy-side firms, being able to demonstrate to their clients that they have effective risk management and trader surveillance systems in place is a commercial differentiator.

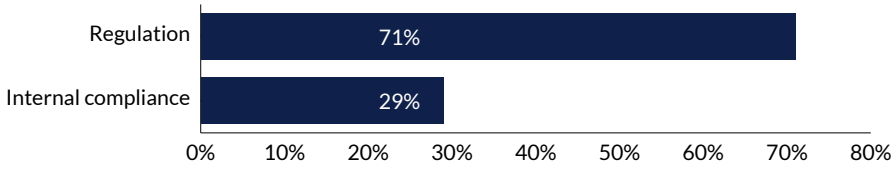
In managing trader surveillance, FIs can address two related areas:

- **Regulatory compliance**. Regulators often provide specific guidance and minimum standards covering the risk of market abuse and how to monitor it.

- **Internal compliance**. FIs define policies and procedures to protect themselves from the adverse effects of abuse (such as damage to their reputation and performance).

According to our survey, **most trader surveillance is still driven by regulation** rather than by internal leading practices and business requirements (see Figure 2).

Figure 2: What is your adoption of trader surveillance systems primarily driven by?



N = 21 FIs
Source: Chartis Research (Global Trader Surveillance Survey, 2017)

Stricter regulations

FIs view regulatory requirements (such as those mandated by the Market Abuse Directive II [MAD II] and MAR in Europe, and the Commodity Futures Trading Commission [CFTC] and the Securities and Exchange Commission [SEC] in the US) as, if not leading practice, then at least a more concrete way to assess trading behaviors such as layering and spoofing[5]. Certainly, FIs can't afford to ignore the regulators: institutions on both sides of the Atlantic have been fined for algorithmic trading abuses[6 7] and OTC derivatives[8] manipulation. And the personal consequences for violations have also become more severe – up to and including imprisonment.

In Europe, the Market Abuse Directive (MAD) was adopted in 2003, and was designed to build an EU framework for tackling insider dealing and market manipulation. It was strengthened in 2014 with the introduction of the MAR and a new Directive on Criminal Sanctions for Market Abuse (CSMAD). The scope of the regulation means that while there is a European focus, international firms with significant presence in European markets must also manage their MAR compliance. REMIT, meanwhile, focuses solely on energy trading firms, and – like MAR – defines and prohibits multiple forms of market abuse.

[4] *See the Chartis report* Spotlight on Trade Surveillance in Energy Trading *for more detail.*
[5] *When spoofing and layering, traders attempt to create the misleading impression of large numbers of orders by placing orders with no intention of executing them.*
[6] ***https://www.fca.org.uk/news/press-releases/fca-fines-us-based-oil-trader-us-903k-market-manipulation***
[7] ***http://www.cftc.gov/PressRoom/PressReleases/pr6649-13***
[8] ***http://europa.eu/rapid/press-release_IP-16-4304_en.htm***

In the US, several regulators have the ability to investigate or prosecute market abuse, including the Department of Justice, the New York State Department of Financial Services, and the Federal Bureau of Investigation. But two bodies in particular focus predominantly on market abuse and trader surveillance:

- The CFTC oversees commodities and related financial instruments on regulated exchanges, as well as swaps. It also polices the trading of commodities, including financial instruments.

- The SEC oversees the trading of stocks and bonds.

The SEC has traditionally been more powerful and strict in its handling of market abuse. Arguably, however, the CFTC has overtaken it of late. In 2016, updates to the Dodd-Frank Act gave the CFTC extra powers to address violations in which defendants were found to have acted 'recklessly' (rather than with intent)[9]. The update also included a rule covering 'manipulative or deceptive devices', which enabled the CFTC to target illegal use of MNPI. This widening of capabilities has made targeting violations much easier, and has enabled the CFTC to levy more industry fines (more than $3 billion in 2016 alone[10]).

Regulatory lock-in

Industry guidance[11] has been used to define scenarios such as front-running, churning, wash trades[12] and spoofing. From one perspective, FIs benefit little from working outside the regulators' definitions and examples. In other words, from the standpoint of the institutions themselves, beyond simply achieving compliance, where is the tangible *business benefit* in capturing new emerging behaviors? The business case is harder to prove, so for many FIs, the benefit of an effective trader surveillance system is largely in proving to clients, stakeholders and regulators that they are managing their risks. And litigation from clients, and the high costs associated with treating customers unfairly, have become more prevalent issues.

This has created a locked-in environment. To ensure they march in unison, FIs have historically tended to employ the same systems and analytics as their peers, and as the regulators. In asset classes that have been subject to regulation for longer (equities, for example), this has led to stagnation: until recently there has been neither pressure on FIs, nor much of an incentive, to improve their systems. And the more clearly defined the concepts of market abuse become, the more easily a determined unethical trader can work around them. The problem with such a rigidly defined approach is that it can be exploited until it is no longer managing risk in any real sense – identifying false positives where there is no abusive activity, while 'unknown unknowns' (e.g. types of market abuse that legacy rules-based systems cannot capture) happen elsewhere, effectively out of sight.

However, as the regulators' priorities have shifted, mandating a wider focus on asset classes[13] and trading venues[14], so has the status quo. In addition, thematic reviews and regulatory attention over the past five years have increasingly driven FIs to consider the risks across fixed-income, currencies and commodities. And, as our survey shows, many FIs are aware of the importance of internal compliance: 29% of them prioritized it. Individuals in FIs are becoming more accountable for areas such as the front office, driving firms to innovate and develop their surveillance capabilities. The upshot of all this is that FIs must establish their own leading practices.

[9] ***http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2011-17549a.pdf***
[10] ***http://www.cftc.gov/PressRoom/PressReleases/pr7274-15***
[11] *Such as the Fixed Income, Currencies and Commodities (FICC) Market Standards Board FX surveillance good practice guide, ESMA's technical standards and the FX Global Code.*
[12] *Front-running occurs when a trader deals based on confidential advance information. Churning occurs when a trader performs excessive trading to maximize their commission. Wash trades occur when an individual trader buys and sells an asset simultaneously, which can give a misleading view of the interest on that asset.*
[13] ***http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:145:0001:0044:EN:PDF***
[14] ***https://www.fca.org.uk/mifid-ii/4-organised-trading-facilities-otfs***

3. Current state: highlighting the ABCD of trader surveillance

FIs' capabilities and requirements are evolving, but the current state of trader surveillance is defined by a range of issues, a variety of approaches, and a great deal of confusion.

To assess the effectiveness of their trader surveillance systems, FIs should consider four main success factors:

- The **Accuracy** of their trader surveillance systems.
- The **Breadth** and depth of their trader surveillance coverage.
- The **Culture** and organizational approach they take to trader surveillance.
- The **Data** they are managing – which underlies all their systems and processes.

Only by asking themselves some key questions in each of these areas can FIs properly address the issues at hand and move forward.

1. **Accuracy** – *is our current solution efficient, effective and accurate?*

There are two basic reasons for inaccuracy in a trader surveillance system:

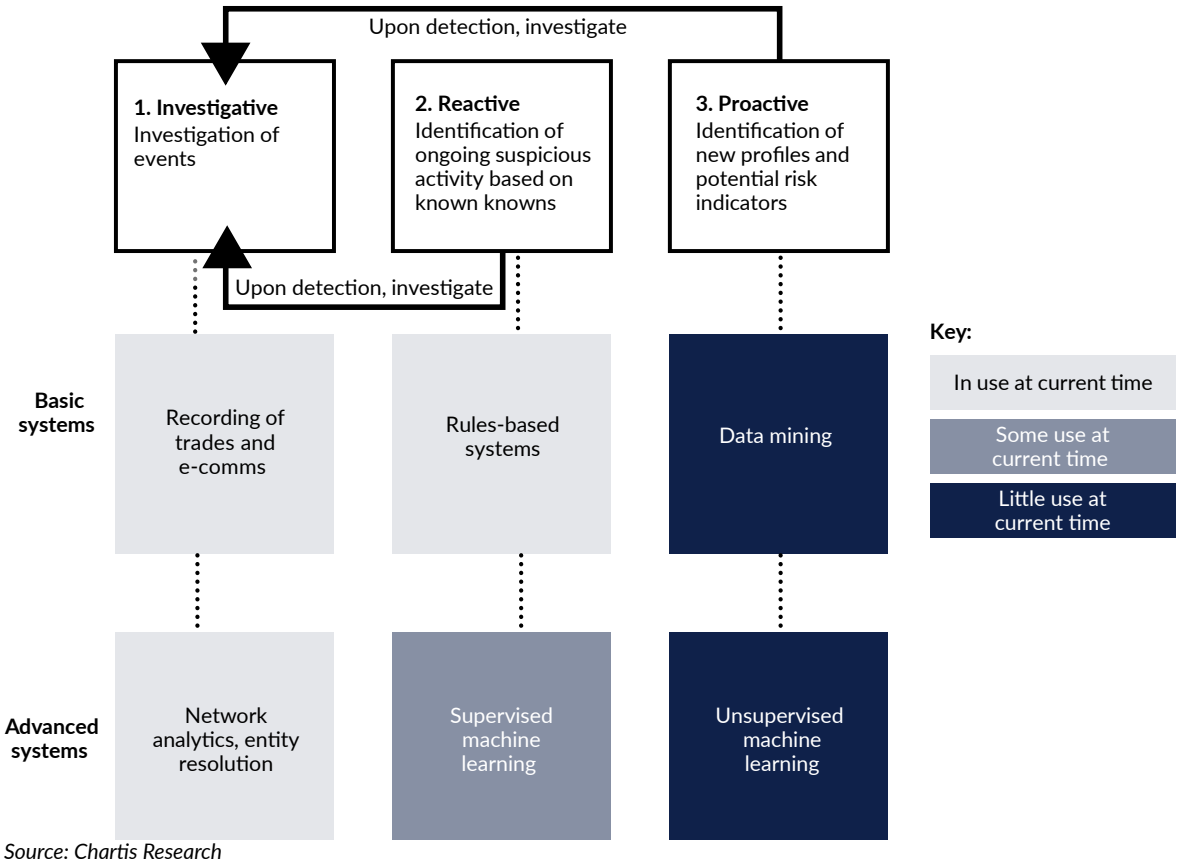
- Failures in *design* (for example, simple control logic picking up too many false positives and/or overlooking acts of misconduct).
- Failures in *implementation* (for example, the system picks up a relevant event but other problems, such as data issues, reviewer error, or a failure to escalate, prevent the FI from addressing the issue).

To answer the accuracy question, FIs need to consider the underlying risks that trader surveillance needs to mitigate – the reasons why the system is in place. This can be broken down into two areas: **detection** and **investigation**.

Detection

- **ISSUE 1: Current systems use *reactive*, post-trade controls, but have no *proactive* approach**. Proactive systems, which can identify new profiles and risk indicators before market abuse incidents happen, are underused, even in more technologically advanced FIs (see Figure 3). These systems include advanced data mining techniques, such as topographical analysis, and unsupervised machine learning, which can be used to determine new clusters of behavior, and risk indicators.

Figure 3: The evolution of investigative, reactive and proactive surveillance

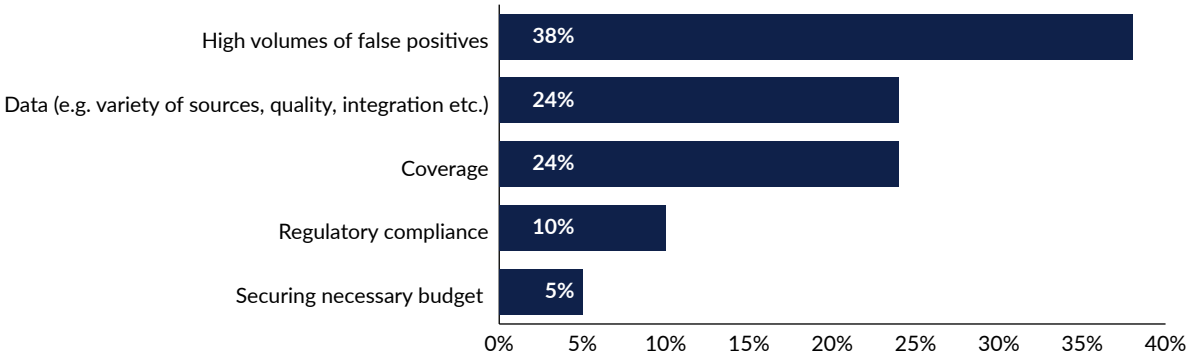


Source: Chartis Research

- **ISSUE 2: It is difficult to qualitatively determine success**. In an environment where 'noise' often drowns out 'signal', what counts as market abuse? A strange-looking trade may indicate insider trading, or it could simply be the result of a trader playing an uncharacteristic hunch. Many alerts are generated daily, but few lead to anything significant. FIs are therefore left with large numbers of low-quality 'false-positive' alerts to process, leading to Issue 3.

- **ISSUE 3: The challenge posed by large numbers of false positives**. The issue of handling false positives is a critical challenge for FIs (see Figure 4). Systems can process 10,000 alerts a day, without revealing even one 'true' positive, and processing them is costly and inefficient. All of which underlines the strong correlation between good data and good outcomes (the importance of acquiring and processing good-quality data is explored later in this report).

Figure 4: What is your greatest surveillance challenge?



N = 21
Source: Chartis Research (Global Trader Surveillance Survey, 2017)

Investigation

- **ISSUE 1: Investigation is costly and time-consuming**. FIs will often use many FTEs to trawl through large volumes of ineffective alerts.

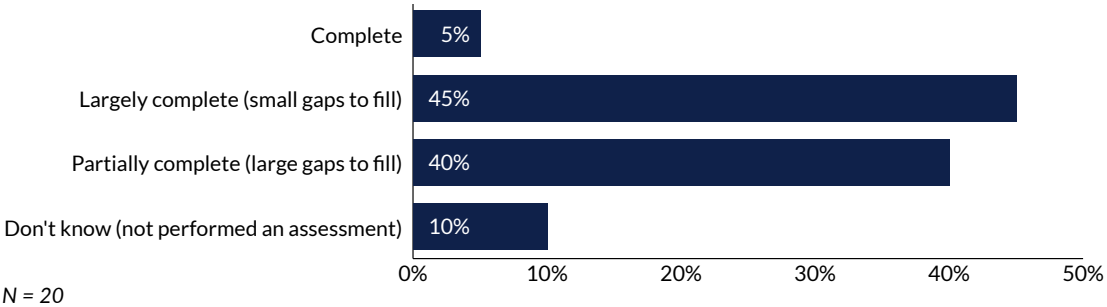
- **ISSUE 2: There is little or no drill-down**. FIs' data interrogation capabilities are often not flexible enough to analyze the underlying metadata and associated information around trades and communications.

2. Breadth and depth – *are we adequately covering our material risks?*

Vertical coverage – assets and geographies

- **ISSUE: Few FIs' surveillance systems cover their asset classes and geographies fully**.[15] According to our survey, only half of respondent firms reported complete (5%), or near-complete (45%), asset class and/or geographical surveillance coverage (see Figure 5). And, as Figure 4 showed, achieving optimal surveillance coverage was called out as a significant challenge by about one in four respondents.

Figure 5: How complete is your surveillance across the asset classes and geographies in which you operate?

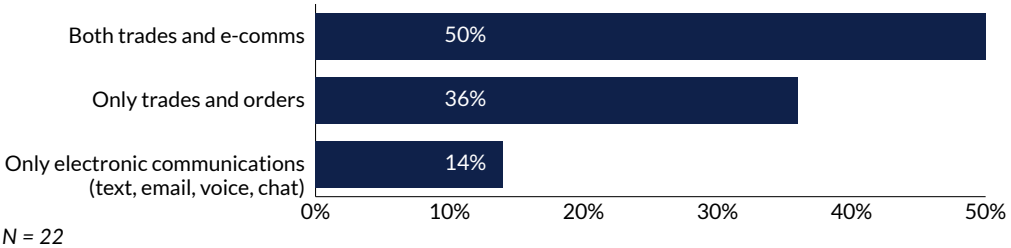


N = 20
Source: Chartis Research (Global Trader Surveillance Survey, 2017)

Horizontal coverage – trades and e-comms

- **ISSUE: Most firms do not have holistic surveillance**. We can define holistic surveillance as bringing together trade, written and voice communications data, and other relevant data points, to create an integrated picture of an FI's activity. In our survey, only half of FIs claimed to be monitoring e-comms as well as trades and orders (see Figure 6). This increased to 60% among Tier 1 respondents (N=5).

Figure 6: What data sources does your trader surveillance system monitor?



N = 22
Source: Chartis Research (Global Trader Surveillance Survey, 2017)

[15] *It is possible that the significant proportion of Tier 3 FIs in our survey sample may be weighting the results here. However, while Tier 1 firms tend to have much greater breadth of coverage and more complex systems, those FIs that considered their coverage to be 'complete' were Tier 3 organizations. Notably, no Tier 1 FIs (N=5) considered their coverage to be 'complete.'*

It is much harder to investigate an alert if the communications around the relevant trade cannot be easily analyzed. Most FIs use their e-comms monitoring systems as a 'box', where communications go into data storage and are only analyzed if a separate compliance issue emerges, either because of outside pressure, such as an external scandal, or because of a suspicious trade alert. Even in those cases where FIs are monitoring both types of information, they are not monitoring e-comms 'in-flight' for trades, making preventing abuse much harder. This is often the case even if those FIs use trade and e-comms on a common platform – they will still largely be used as separate capabilities.

There are a number of possible reasons for this – not least the relative immaturity of e-comms detection capabilities. Text mining capabilities and lexicons of market abuse terminology are relatively simplistic and can be worked around with ease. Combining the data and analytics from these systems with trade monitoring systems creates extra difficulty, because it can be hard to establish quantifiable Key Risk Indicators (KRIs): which terms in a chat should be flagged, for example, and in which combinations? And how can that score be combined or compared with other trade monitoring scores?

Using trade and order monitoring systems, FIs or regulators can identify areas that may need further investigation. But these systems do not take account of the motives behind trades, which may be perfectly legitimate – often, it is the communications around trades that provide investigators with their 'smoking gun'. Furthermore, in market abuse cases, both types of evidence are typically needed: *mens rea* (intent/mental state) and *actus reus* (the action itself).

3. Culture and organization – *do we have a culture of effective accountability?*

- **ISSUE: Better analytics and broader coverage are ineffective unless they are embedded in appropriate governance structures**. With a large volume of reports and false positives, FIs risk creating a culture in which alerts are closed quickly without being reviewed, rather than one that ensures a fair and orderly process of analysis and response.

A culture of confusion – the evolving three lines of defense

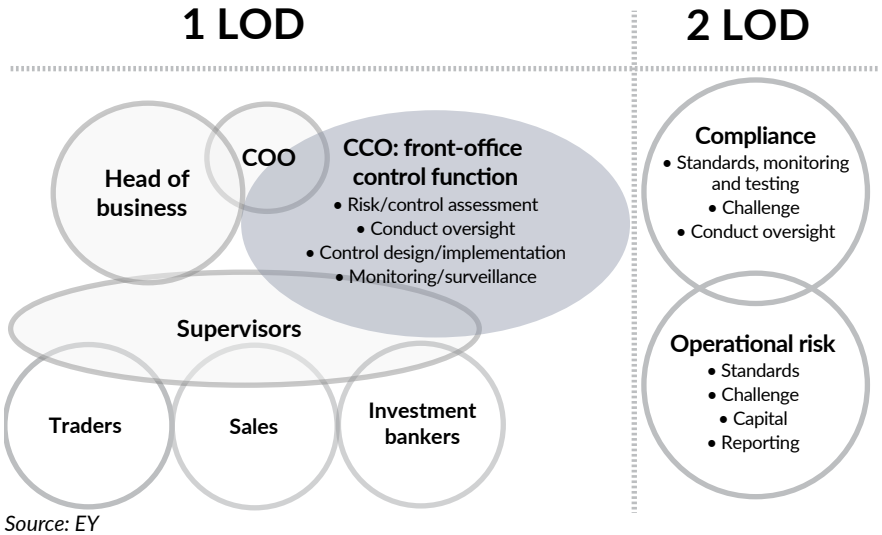
The established three lines of defense (LOD) model, and the overall control environment, are evolving. Increasingly, the first line of defense control function drives the control agenda and assesses the value of individual controls.

At the same time, the second LOD is moving away from running controls itself to setting the standards for control and control assurance that the first line must meet – as well as overseeing, testing and challenging the first LOD's activities. As this trend continues, confusion will naturally arise about the role of each LOD, intensifying as the overlap between the activities and responsibilities of each grows.

This is a challenge for FIs, because the ways in which LODs interact should be enhanced and streamlined rather than made more complex. The process of evolution can be eased, however, if FIs develop an operating model based on their activities; one that is agreed by all three LODs together. In this it is vital to clearly outline risk and reward, and the activities that belong in each line should be governed by principles of accountability and independent challenge (see Figure 7).

These can be fed and enabled by centralized outputs and case management*, which deliver high-volume alerts to the first line, and deep-dive analysis capabilities to the second. More holistic information delivered within a well-defined framework of responsibilities can enable firms to move beyond box-ticking compliance to a more insightful and engaged culture.

Figure 7: The evolving roles of the first and second lines of defense for trader surveillance



Source: EY

**As highlighted in Figure 13 on page 24*

4. **Data** – *is our data of high enough quality?*

- **ISSUE 1: Risk systems require good quality data**. Regulators such as the Financial Industry Regulatory Authority (FINRA) have indicated that data integrity controls will feature heavily on their agenda.[16] Systems that rely on rules engines and statistical analysis often require data in a specific format, and good quality data is essential – especially timestamps for trades from different systems (which are often not automatically captured for manually entered or transferred voice-brokered trades). The data that goes into trader surveillance systems must be of a consistent format, and this is especially true when data is being pulled from multiple sources. Automatic feeds and timestamps can also ameliorate one common problem with manually entered trades, which is that they can appear to have occurred seconds, minutes or hours later than they actually did.

- **ISSUE 2: Mapping data across the organization is a complex undertaking, but is necessary for holistic surveillance**. Lists and sub-lists of individuals may be held in a single location, or in several places. And certain lists – such as those used to prepare annual reports and accounts, or to support debt issuance – may be held in centralized HR systems. Others may be held in corporate banking, investment banking and market divisions, and are often transaction-specific. Devising a reliable way to map all the relevant data needed for trader surveillance purposes, and then keeping these maps updated, could be a major challenge.

- **ISSUE 3: Handling Big Data**. FIs also face a considerable challenge in finding ways to query and surface the data they need from across an increasingly varied and amorphous data environment. The e-comms data that FIs process, for example, can come in relational, structured formats (typically in row-and-columnar databases), semi-structured formats (e.g. weblogs, social profiles and XML), or completely unstructured formats (e.g. images, audio or pdf documents).

[16] ***http://www.finra.org/industry/2016-regulatory-and-examination-priorities-letter***

4. Future state: tackling the issues

Emerging themes and solutions – how can FIs address these issues?

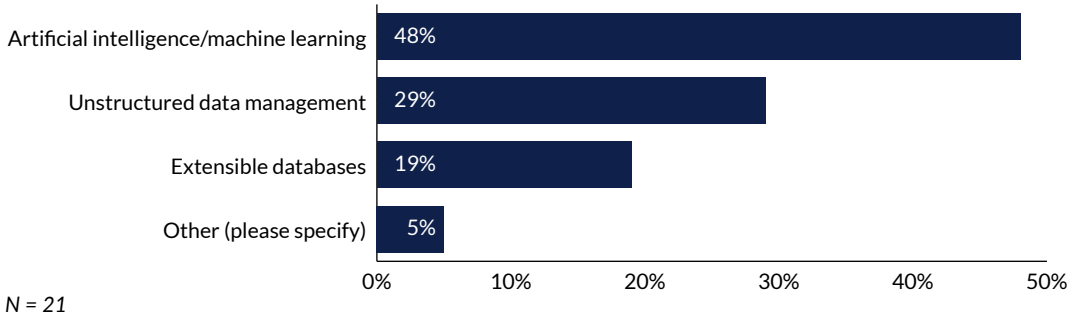
1. Analytical accuracy

Better detection

FIs can address the need for greater accuracy with **more accurate analytics, to generate fewer, better quality alerts**. Solution vendors are addressing these requirements with machine-learning algorithms, adaptable model-building solution sets and behavioral analytics, to detect anomalies more accurately and match them against 'normal' trader behavior. Combining e-comms and trade monitoring signals can provide fewer, better alerts. Criteria chains[17], for example, can ensure that only the most important alerts are passed for analysis.

The expanded coverage of trader surveillance has driven a corresponding expansion in systems and data. For respondents in our survey (see Figure 8), the primary technology priority was Artificial Intelligence (AI)/machine learning. (Among Tier 1 respondents [N=5], the proportion that considered AI to be a priority increased to 80%). Unstructured data management goes hand-in-hand with AI, because of the close links between the two (e.g. unstructured data can be parsed with machine-learning algorithms to provide more comprehensive alerts).

Figure 8: What do you consider to be a technology priority for trader surveillance?



N = 21
Source: Chartis Research (Global Trader Surveillance Survey, 2017)

AI and machine learning can generate more accurate analytics. Supervised machine learning can be used to tune existing reactive systems to provide better alerts. According to some subject matter experts, using machine learning and unstructured data analysis has reduced false positives by as much as 50%, generating Returns on Investment (ROIs) of more than 60% (in terms of FTE-related savings). And, importantly, unsupervised learning can also be used to uncover the 'unknown unknowns' that can help systems develop more preventive functionality.

Better investigation

Advanced workflow and automation processes are providing better alerts management. This could include using more advanced workflows to determine whether alerts are passed to more sophisticated investigation teams, or completely automating certain areas of the workflow instead. In the latter case, the overall number of alerts is not dramatically reduced, but the use of advanced workflows,

[17] *Criteria chains ensure that all relevant criteria must be met before market abuse is flagged. Systems can then be set up to produce fewer overall alerts, significantly reducing the number of false positives.*

and potentially RPA, could certainly reduce employees' workloads, and eliminate false positives more quickly.

Many advanced investigation techniques focus on resolving relationships between individuals. FIs could use entity resolution and network modeling systems, for example, to capture the underlying metadata of communications between traders, and to identify potentially risky networks of individuals. Most current solutions are simple networks with relatively crude connections. But they can be made more sophisticated using enhanced relationship extraction (such as communications sentiment analysis) and social network analysis (i.e. peer-grouping and baselining behavioral networks).

2. Broader coverage

Asset class coverage

Increased regulatory and technical incentives are pushing FIs to invest more in real-time responsiveness, calculation curves, multi-factor pricing and limits management. These include intraday limit monitoring for market risk and unauthorized trading risk mitigation, and monitoring algorithmic trading activity for compliance with MiFID II. From a technical perspective, it is now possible to provide capabilities such as real-time xVA simulations for derivatives in near real-time, to provide intraday data to inform trading decisions.

Trader surveillance vendors have also been investing in direct data feeds for equities, derivatives and options markets, and have been focusing on integrating derivatives and underlying financial instrument data as quickly and efficiently as possible. They are also addressing issues around the time and cost involved in integrating systems, and possible overruns, by making their solutions as 'out of the box' as possible. This is often viewed as more of a concern for Tier 2 and 3 institutions, which tend to favor simpler systems for a lower price. But the complex bureaucratic and technical structures of Tier 1 FIs can make quick implementations appealingly simple. However, in more complex asset classes (such as fixed-income and commodities) it can be difficult to achieve the desired flexibility.

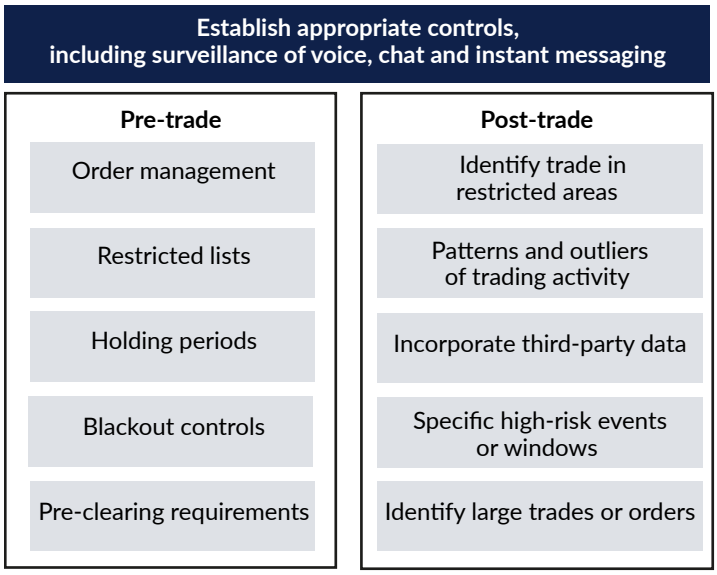
There is a focus on low-latency reporting and time-series databases that use higher data-processing speeds to handle the greater volume and velocity of trades and orders in areas such as dark pools and algorithmic trading. Incumbent technology vendors are struggling to provide these capabilities, creating an opportunity for new vendors that could then be positioned to become the industry standard. Several banks are also developing in-house systems to monitor these areas.

Horizontal coverage: e-comms and transactions

Solution vendors are attempting to synthesize e-comms and trade monitoring into a single process, either by integrating their solutions with separate e-comms monitoring systems, or by integrating e-comms systems from other areas of their product stack. Most of these solutions are still text-mining emails, chat and text tools, but some vendors are focusing on voice analysis capabilities.

But to achieve the holistic focus they need, FIs must more effectively monitor e-comms that coincide with suspicious trading alerts, to determine if flagged traders have started communicating in suspicious ways. As semantic analysis, text mining and voice recognition become more effective, and analytics become ever more advanced, more FIs will be able to generate alerts based on a richer combination of signals, across e-comms and trade monitoring, to generate better results (see Figure 9).

Figure 9: Examples of pre- and post-trade controls



Source: Chartis Research

SCENARIO: To create market movement, a trader submits a large number of orders that are rapidly canceled, then executes a trade on the opposite side of the order book, indicating spoofing activity.

The alert generated will be stronger if:

- P&L information, market data, position and order book re-creation reinforces the indication of trading on both sides. This is the focus of most current surveillance systems.
- E-comms monitoring detects the use of language that indicates the trader may be deliberately attempting to manipulate the market (although issues around privacy mean that not all firms monitor the content of communications).
- Metadata links them to another trader attempting to capitalize on the effects of those suspicious cancellations (i.e. one who trades on the market movement generated by the trader in the first scenario). Analyzing communications metadata has an advantage in that it is less intrusive than monitoring communications directly.
- Repeated patterns of behavior are detected – a single occurrence of anomalous behavior can be a coincidence, but a pattern indicates intent. A system can then move from investigating individual alerts to a more holistic view of a trader's activity.

Unstructured data management systems

The need for in-flight e-comms analysis has fueled a drive toward semantic database management systems, which can handle unstructured data sets and search large volumes of information. NoSQL (or NoREL) databases are becoming increasingly popular, and applications such as Hadoop are often used to provide a suitable software framework. Many Tier 1 institutions are undertaking multi-year projects to migrate their key systems to non-relational databases. The vendors supplying them are attempting to keep up with this trend by ensuring they can integrate their solutions with unstructured databases, or provide their own.

This approach will enable a **holistic view of requirements** that accounts for FIs' asset classes and their trade and e-comms monitoring. However, to monitor activity across both areas, FIs will need a centralized data repository. They could, for example, capture the trades around both equities and equity options in a single solution, to determine whether a trader is using underlying instruments to influence the option. They could also use e-comms data, in combination with transaction information, for both reactive and proactive monitoring.

Case study: understanding the language of e-comms

A global Tier 1 investment bank recently made a substantial upgrade to its surveillance and monitoring capabilities. The objective of the project was to enhance the bank's existing technology solutions and processes to meet increasing regulatory expectations, and to improve the efficiency and effectiveness of its surveillance by:

- Reducing false positives.
- Optimizing and contextualizing alerts using advanced techniques (such as combining structured data or alerts with unstructured data).
- Using emerging techniques such as Natural Language Processing (NLP), machine learning and advanced analytics.

An initial analysis of the bank's regulatory requirements and expectations detailed the end-to-end aspects of e-comms monitoring across the bank's functional, technical and generic requirements. This determined that its current surveillance techniques were both ineffective and inefficient. Following a vendor selection process a Proof of Concept phase helped to identify emerging techniques to reduce false positives and identify true risks. These included:

- Applying metadata-driven business rules.
- Excluding mass communications (e.g. newsletters, spam, internally published reports, or system notifications).
- Combining additional data sources (e.g. wall-crossed or insider-identified individuals and events, and alerts from trader surveillance systems).
- Using NLP analytic engines to identify behavior based on language (e.g. secrecy, price manipulation) and context (e.g. business, personal, business as usual) through several iterations.

To achieve the desired precision, data scientists trained the NLP engines using several test data sets, and trained and tested different NLP/machine learning layers over a number of iterations.

The result was a successful migration from a simple keyword-based surveillance system to a robotic and cognitive system with contextual understanding and an ability to predict. The bank can now identify suspicious communications more accurately and at lower cost.

3. A more accountable culture

Surveillance should be built into an FI's conduct and risk agenda, with clearly identified lines of ownership for those in the surveillance and compliance functions.

This can be challenging, because recognizing the commercial advantage of better surveillance is difficult. The exploratory analysis of emerging threats and compliance errors can be difficult to map against historic threats. FIs must be able to demonstrate to regulators that their systems and controls are effective, while still trading profitably.

Most front-office dashboard solutions are still limited in scope and cumbersome to run. In practice, FIs will also have to invest heavily in solutions that can offer more holistic and automated systems for data gathering, analysis and reporting (see Figure 10). And trader surveillance systems will have to integrate with GRC and operational risk frameworks and external controls to deliver more quantifiable conduct data about their traders.

Figure 10: Processes and technology for cultural monitoring

Focus area	What it entails	Tools and technologies
Process control and process analytics	• Risk assessments • Process and process analysis	• Control software • GRC and operational risk frameworks • Training software
Analytics	• Operational analytics • Incentive plans and analysis • Strategy and appetite analysis	• Statistical models and frameworks • Causal analytics for operational risk and process analysis • Product risk analytics
Evidence and records management	• Recording available transaction data, including public data • Internal communication and transactional records • Internal planning, HR and operational records	• Communication archives • Big data technologies (e.g. Hadoop, Spark etc.)

Source: Chartis Research

Technology solutions can provide effective benchmarking and feedback mechanisms. GRC systems provide a baseline for these capabilities. To integrate conduct risk into FIs' business strategy, solutions can dynamically link quantitative and qualitative data, and use advanced pattern recognition analytics and workflows.

FIs will also have to determine how much information is delivered to traders. So, for example, advanced reporting and e-learning tools could be made available to traders so they can benchmark themselves with a simple user-generated 'my surveillance score'. Such tools, driven from data captured through day-to-day surveillance activity, could be used to drive a culture of personal accountability.

4. Better data

FIs should consider solutions to manage the integrity of business data and the associated control processes throughout their lifecycle. Solutions should be able to provide:

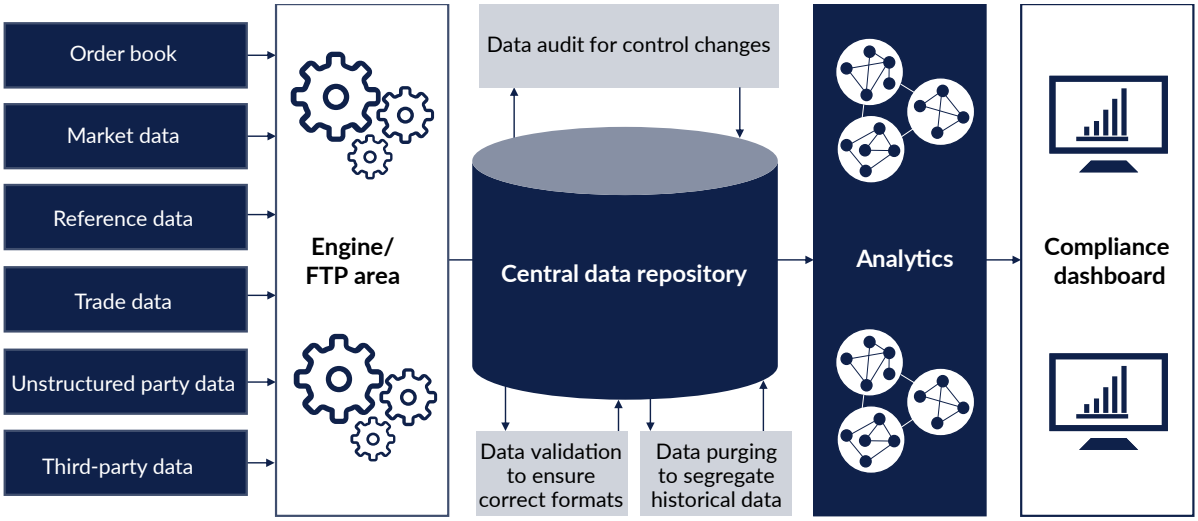
- An audit record of when the control was introduced, and any subsequent amendment to its configuration.
- An audit record of the results of the control, including how often it was used and whether any deficient control activity was fixed.
- The ability to archive and purge data control results and associated data in line with corporate retention policies.
- The ability to validate data to ensure that formats are correct.

This should be available for multiple transactional and communications data formats, such as:

- **Trade data**. Includes counterparty details, execution price, execution date and time, order type and exchange.
- **Market/third-party data**. The data obtained from exchanges, such as trade volume, day-high and day-low price, and daily market tick price for different securities. The required data may come in multiple formats (such as CSV and MDDL).
- **Reference data**. Including master data information such as customer and security/derivative names.
- **Unstructured data**. Including data such as insider information on publicly traded firms, with insider codes and other identifying information. This includes e-comms and voice data.
- **Order data**. Including instructions to buy or sell a financial instrument at a specified rate, until the order is executed or canceled, making it time-sensitive.

Automated processes can deliver data into a centralized repository and update as necessary (during periods of lower activity, for example). These can provide the audited, validated data necessary to feed risk systems and provide accurate alerts (see Figure 11).

Figure 11: Data validation, audit and purging for multiple data types



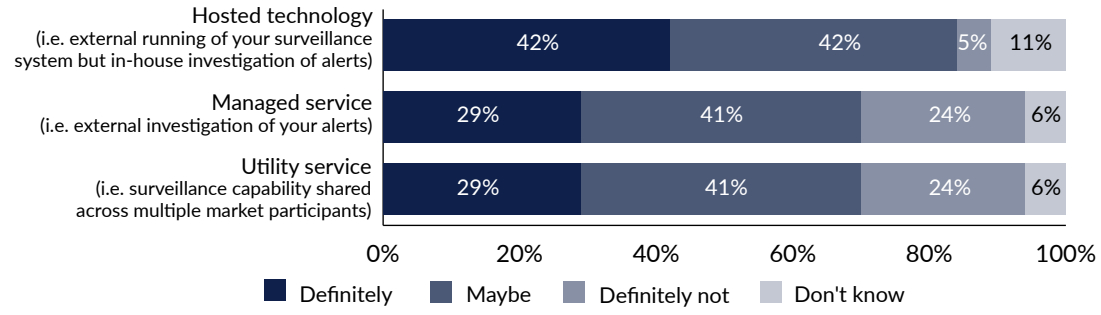
Source: Chartis Research

For most firms, however, this unified architecture currently represents an aspiration rather than a reality – they may not be able to build data lakes or take the time to restructure their silos. However, there are solutions that can move data into analytics or dashboards, including abstraction layers to link processes, or knowledge graphs to recognize links between different metadata components. These can be valuable tools for FIs integrating data feeds without constructing a perfect data architecture first.

Externalizing the issues

If FIs *are* improving their systems, how are these projects proceeding? One development we are seeing is the emergence of externalized, vendor-driven, front-office risk systems, in both buy-side and sell-side firms. The concept of embedded risk management in trading systems is breaking down, and in many cases current risk systems are becoming increasingly redundant. Externalized, vendor-sourced risk systems are less costly, more flexible and easier to manage, and help buy-side firms advertise the effectiveness of their risk management to potential clients. This was highlighted in our survey – while FIs were largely uncertain about whether they would use outsourcing for trader surveillance, 42% indicated that they would 'definitely' consider using hosted technology (see Figure 12).

Figure 12: Would you consider any of the following outsourcing options?



N = 19
Source: Chartis Research (Global Trader Surveillance Survey, 2017)

5. Taking stock: so, what is the future of trader surveillance?

Table 1 summarizes the key challenges, solutions and benefits in achieving successful trader surveillance within the ABCD framework.

Table 1: Taking on challenges; moving to the future

Issues		Challenges	Addressed with	Future benefits
Accuracy	Investigation	Lack of detail in relationships between traders and across trades	Network analytics, hierarchy modeling and entity resolution	More insightful views of traders, counterparties and stakeholders
	Detection	High volume of alerts	RPA, workflow engines, supervised machine learning	Lower FTE burden; analysts can spend more time on meaningful alerts
		Backward-looking analytics	Natural language processing, unsupervised learning, criteria chains	Revealing more insightful alerts, and detecting alerts that are missed by traditional methodologies
Breadth	Asset classes and trading venues	Limited coverage, no cross-asset analysis	Integrated Big Data with cross-asset analytics	Unified, holistic view across assets and communications
	Data types	Limited integration between e-comms and transaction and order data		
Culture		Culture of closing alerts quickly rather than examining the underlying factors	Tangible conduct risk outcomes via dashboards and processes	More informed employees, delivering understandable and quantifiable results to key stakeholders and the board
		Lack of structure, difficulty in recognizing improvements		
Data		Inaccurate data, without interrogation capabilities	Data integrity and control, cleaning and validation	More accurate, verifiable information delivered at every stage of the process

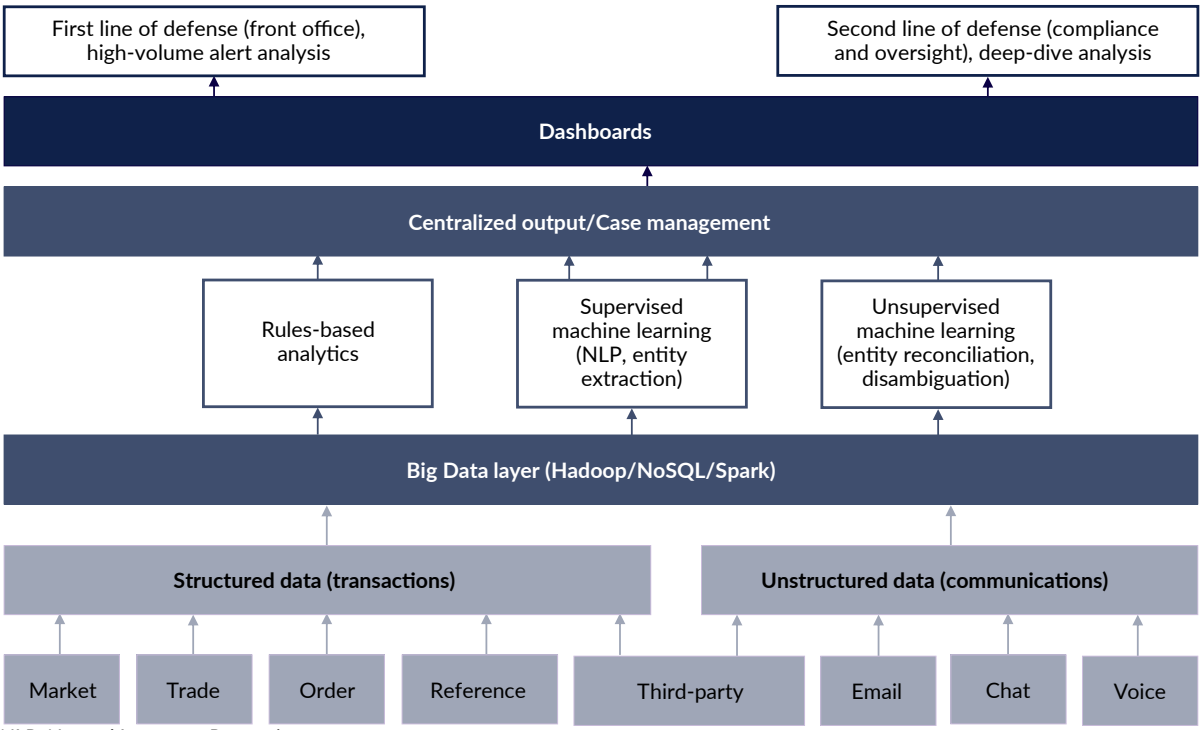
Source: Chartis Research

Most of the increase in spending in the sector is likely to remain tactical, focused on extending existing point solutions – including enhanced analytics and out-of-the-box reporting – or buying new ones. At the same time, there is also likely to be a low volume of very high-value transformational projects. These are likely to be undertaken by organizations in the upper-Tier 2/Tier 1 levels, which are seeking economies of scale.

These solutions will be complex, and the future of trader surveillance – with integrated conduct risk, advanced analytics, extensible databases, and integrated e-comms and trade monitoring – might seem complicated and difficult to implement. Nevertheless, FIs can develop a path toward the future by prioritizing certain elements and identifying specific solutions.

A target trader surveillance architecture should be able to deliver unified trade monitoring and e-comms monitoring data to the first and second lines of defense (see Figure 13). This can be developed through phased, modular enhancements, beginning with basic data integrity and control processes. A system covering each of these areas can then provide a centralized data repository to manage additional related data, including conduct risk data, HR data, and P&L data.

Figure 13: Potential holistic trader surveillance architecture



NLP: Natural Language Processing
Source: Chartis Research

Conclusion

As our survey shows, firms struggle to provide effective monitoring of all business lines and requirements, and cultural and governance processes form a vital part of a successful system. The scale and scope of FIs' requirements are expanding quickly, and the need to refresh their technology has become more pertinent in recent years.

Trader surveillance budgets and expenditure may have expanded, but there is no guarantee that their systems will address systemic deficiencies. FIs should work to the ABCD principles to deliver broader, more effective and more efficient surveillance. Their systems should continue to evolve, covering more areas, detecting more breaches of compliance, and generating better alerts.

Ultimately, by linking all the elements and integrating sources of information to leverage more insight, FIs can break down the barriers between the different types of surveillance. They will know their traders, understand their employees, and recognize how they make their profits. Better monitoring

will enable FIs to use highly skilled resources more effectively, by delivering more high-quality alerts to individuals.

Today, trader surveillance is a complex area of an FI's operations. But by addressing the ABCD of surveillance, and adopting the right balance of people, processes and technology, FIs can emerge from the confusion and bring new insight – and value – to the way they work.

6. Appendix A: Global trader surveillance survey

As part of our research and analysis, this report includes the results of a 2017 global survey conducted by Chartis Research. It surveyed 35 FIs about their use of trader surveillance, and the challenges they faced in implementing it.

Of the respondents surveyed:

- 37% were from Europe.
- 23% were from North America.
- 20% were from Asia-Pacific.
- 20% were from the Rest of the World.

- 20% were Tier 1 organizations (more than $100 billion in assets).
- 23% were Tier 2 organizations (between $10 billion and $100 billion in assets).
- 57% were Tier 3 organizations (less than $10 billion in assets).

Additional insight for this report comes from roundtable discussions and interviews with EY subject matter advisors.

7. How to use research and services from Chartis

In addition to our flagship industry reports, Chartis also offers customized information and consulting services. Our in-depth knowledge of the risk technology market and best practice allows us to provide high-quality and cost-effective advice to our clients. If you found this report informative and useful, you may be interested in the following services from Chartis.

For risk technology buyers

If you are purchasing risk management software, Chartis's vendor selection service is designed to help you find the most appropriate risk technology solution for your needs.

We monitor the market to identify the strengths and weaknesses of the different risk technology solutions, and track the post-sales performance of companies selling and implementing these systems. Our market intelligence includes key decision criteria such as TCO (total cost of ownership) comparisons and customer satisfaction ratings.

Our research and advisory services cover a range of risk and compliance management topics such as credit risk, market risk, operational risk, GRC, financial crime, liquidity risk, asset and liability management, collateral management, regulatory compliance, risk data aggregation, risk analytics and risk BI.

Our vendor selection services include:

- Buy vs. build decision support
- Business and functional requirements gathering
- Identification of suitable risk and compliance implementation partners
- Review of vendor proposals
- Assessment of vendor presentations and demonstrations
- Definition and execution of Proof-of-Concept (PoC) projects
- Due diligence activities.

For risk technology vendors

Strategy

Chartis can provide specific strategy advice for risk technology vendors and innovators, with a special focus on growth strategy, product direction, go-to-market plans, and more. Some of our specific offerings include:

- Market analysis, including market segmentation, market demands, buyer needs, and competitive forces
- Strategy sessions focused on aligning product and company direction based upon analyst data, research, and market intelligence
- Advice on go-to-market positioning, messaging, and lead generation
- Advice on pricing strategy, alliance strategy, and licensing/pricing models

Thought leadership

Risk technology vendors can also engage Chartis to provide thought leadership on industry trends in the form of in-person speeches and webinars, as well as custom research and thought-leadership reports. Target audiences and objectives range from internal teams to customer and user conferences. Some recent examples include:

- Participation on a 'Panel of Experts' at a global user conference for a leading Global ERM (Enterprise Risk Management) software vendor
- Custom research and thought-leadership paper on Basel 3 and implications for risk technology
- Webinar on Financial Crime Risk Management
- Internal education of sales team on key regulatory and business trends and engaging C-level decision makers

8. Further reading

- *Financial Crime Risk Management Systems: Market Update 2017*
- *MiFID II Reporting Solutions 2017*
- *Spotlight on Conduct Risk Management*
- *RiskTech 100® 2017*
- *Spotlight on Trade Surveillance in Energy Trading*
- *Data Integrity and Control Solutions in Financial Services 2016*

For all these reports see ***www.chartis-research.com***.