



NICE · ACTIMIZE

Stepping up Conduct Surveillance:

10 Must-Haves for
Success



Introduction

In financial services, surveillance has historically been driven by regulations. In the wake of the financial crisis of 2009, misconduct stemming from widespread FX and LIBOR scandals was a springboard for more regulation. Today, a raft of global regulations – MiFID II, MAR, FINRA’s Rules 2111 and 3110, Dodd-Frank, IIROC 1300, SEC’s Regulation Best Interest, OSC’s Client Focused Reforms, the Financial Conduct Authority’s Senior Managers and Certification Regime (SM&CR) and many more – are focused on the many faces of a common nemesis: misconduct.

But regulatory scrutiny of misconduct isn’t just a US or European phenomenon. In every corner of the world, from North America to Europe to Asia to Oceania – regulators are aggressively pursuing firms with conduct infractions, ranging from rogue trading to suitability breaches. Furthermore, under stringent regulations like the Financial Conduct Authority’s SM&CR, board members and senior managers of a firm can now be held legally culpable for their own conduct and also the conduct of their employees. According to Deloitte’s report [Managing Conduct Risk: Addressing Drivers, Restoring Trust](#), the regulatory focus on conduct is only going to continue to gain momentum.

TABLE OF CONTENTS

The Many Faces of Misconduct	4
The Cost of Misconduct	5
Ineffective Surveillance: A Key Driver of Conduct Risk	6
Seeing the Complete Picture: What Siloed Legacy Technology Can't Do	7
10 Must-Haves for Conduct Surveillance	8
#1. Holistic Approach	8
#2. Automation	9
#3. Comprehensive Coverage	10
#4. AI-Powered Analytics, Natural Language Understanding	11
#5. Anomaly Detection	12
#6. Self-Development Analytics	13
#7. Robust Reporting and Data Visualization	14
#8. Enterprise Risk Case Management	15
#9. Advanced Technology for Virtual Work Environments	16
#10. Data to Link Conduct to Pay to Drive Culture	17
Use Case	18
Learn More	19

The Many Faces of Misconduct

Conduct risk may have formed its roots in regulations, but today it has evolved into something much bigger.

“Unlike trade surveillance, there’s no handbook for conduct surveillance,” explains Anurag Mohapatra, Product Manager for NICE Actimize. “Trade surveillance rules are dictated solely by prescriptive regulations like MAR, but there’s no one way that all firms define conduct risk. Every firm views the scope of conduct surveillance differently.”

Some firms view misconduct as mainly regulatory related; others view it on a much broader scale. “One financial customer I consulted with defined misconduct as any form of non-compliance, whether risk-related, regulatory-related, a violation of trading mandates, HR violations, even missed training,” Mohapatra added.

For all the different ways firms view conduct risk, one thing is clear: there are many faces of misconduct and they are constantly changing. Additionally, firms view conduct and surveillance as inseparable.

According to a recent global survey conducted by NICE Actimize, conduct risk concerns are broad and far reaching, with firms prioritizing regulatory factors like market abuse (83%), suitability (24%), rogue trading (40%), financial crime/anti-money laundering (36%), and employee conflicts (24%) high on their surveillance lists. But surprisingly, a large percentage of firms also now view general employee misbehavior (26%) and inappropriate communications (43%) as key conduct surveillance priorities as well (see Chart 1 below).

This same trend held true in a separate APAC survey with 35% of firms citing general employee misbehavior as a key surveillance priority (see Chart 2 next page).



Chart 1 - What are the most important risks your surveillance function is prioritizing for the next 2-3 years (select top 3)



Chart 2 - What are the most important risks your surveillance function is prioritizing for the next 2-3 years (select top 3)

The Cost of Misconduct

Regulations like the FCA's (SM&CR) are also raising the bar on accountability. Senior managers can now face personal fines, even jail time, for reckless decisions.

But aside from personal liability for managers, misconduct can have severe repercussions for firms. In recent years, [conduct-related fines have totaled in a jaw-dropping tens of billions of dollars](#), which can pale in comparison to the cost of business disruptions, lost productivity and revenue.

Still, when it comes to misconduct, [what companies fear most](#) is the risk to their own reputations.

In a sector where firms are already mistrusted – (a [recent Deloitte survey of 33,000 respondents from 28 countries revealed that banking and financial services was the least trusted sector globally](#)) – headlines of rogue trading and other illegal dealings can still create irreparable brand damage.

Additionally, as societal values change, conduct risk is transitioning from something

that's purely regulatory driven to something that's more culturally engrained within organizations. Simply put, conduct is essential to building trust and supporting sustainable growth in today's society.

As a result, conduct has been moving up the compliance agenda. This has been especially noticeable on the buy-side, where increasingly, investors are specifying that they only want to invest in funds which focus on or are offered by companies that behave ethically. As firms aspire to more ethical behavior, conduct surveillance can bring much needed transparency.

Paul Cottee, Director, Compliance Line of Business at NICE, concurs: "We are seeing a dramatic rise in ESG and good corporate-citizenship in general being on companies' radar screens. Not only do they want to avoid the immediate bottom-line hit from a fine, but longer-term, society at large is becoming far less tolerant of companies which are seen to be doing 'the wrong thing' and consumers are increasingly exercising their sovereignty. Culture has to be demonstrated from the top."


Ineffective Surveillance: A Key Driver of Conduct Risk

According to Deloitte's report [Managing Conduct Risk: Addressing Drivers, Restoring Trust](#), despite all the promise of conduct surveillance, ineffective and weak surveillance systems are a key driver for perpetuating conduct risk.

[The report states](#): "If monitoring and surveillance is nonexistent or inadequate, misconduct can go undetected and risks may not be appropriately managed. Further, some individuals may be more likely to engage in poor behaviors because they estimate their chance of being discovered as low."

In addition, [the report](#) went on to point out that "... if systems for monitoring and surveillance are inadequate, management information on conduct will likely be lacking, leaving leadership unable to identify and manage important risks."

In other words, it's impossible to manage risks that you cannot effectively identify in the first place.



"It's impossible to manage risks that you cannot effectively identify in the first place."

Seeing the Complete Picture: What Siloed Legacy Technology Can't Do

With remote and hybrid-remote work environments now the norm, monitoring for conduct risk has never been more necessary.

Still, legacy surveillance technology and practices don't make it easy.

One common conduct surveillance roadblock financial services firms face with legacy systems is the inability to analyze and link data across surveillance and other organizational silos.

This makes it difficult for firms to proactively monitor for conduct issues, and to really get a big picture view. Firms might be able to identify where an individual trader generates a lot of trading alerts, or whether a financial advisor has too many suitability breaches. But at best, this means firms can only achieve a piecemeal view of conduct, at specific, unconnected moments in time.

For example, a credit department might identify that a trader, who we'll call John, has breached his credit limit. HR might know John has repeatedly missed required training sessions in recent months. A separate risk department might see that John has breached his risk limit, and another department responsible for

monitoring complaints might identify John as a risky employee too. But none of these departments know what the other departments know. And worse, because all of the various risk data isn't consolidated or readily available up the chain of command, no one, not even John's direct manager, or the next level executive, or the one above that, truly knows just how much of a risk John is to the firm.

The problem is, for most firms, risk data and alerts are stored in different formats across multiple systems, making it very difficult for managers to get a big-picture view of what's happening with individual employees across the organization.

The FCA affirms that viewing conduct risk in this "diffused way" is a poor practice.

"None of this is particularly new," explains Cottee. "There have been prosecutions in several jurisdictions where investigators have brought together diffused strands of evidence, none of which by themselves is a smoking gun, to create a compelling case. However the joined-up thinking only took place after something else had piqued the investigator's interest."

"The joined-up thinking only took place after something else had piqued the investigator's interest."



10

Must-Haves for Conduct Surveillance

1. Holistic Approach

To understand true risk, you need to look at an individual across multiple dimensions and recognize how that person's risk is evolving over time. But you can't do this if you are operating surveillance in silos.

According to PwC, this is a common problem for many financial services firms today. [This PwC blog](#) espouses a different vision for the future of Market Abuse surveillance, one that "reflects the trend towards a broadening remit of surveillance and integration of conduct-focused monitoring." The blog points out that today, "across the industry, conduct monitoring activities are performed very differently, with supervision teams, Compliance, Surveillance and Control Room monitoring different aspects of conduct. Some organizations are exploring how to bring these together to create a richer view of behavior and more trader-centric monitoring."

In other words, to get to the heart of employee conduct, organizations have to look at more than markets surveillance. In our example of John the trader, the firm will not only need to look for instances of potential market abuse, but will also need to look at whether John is getting complaints from clients, and meeting his best execution obligations. Is John's recent P&L vastly different from the past? Has he been sending risky communications?

To create a complete 360-degree view of John's risk, the firm needs to bring all of the feeds from its different surveillance systems and data sources together.

This points to the need for holistic conduct surveillance.

A holistic conduct surveillance platform consolidates conduct risks across your organization by applying machine learning and behavioral analytics to analyze and link data across various systems, including: Trade Surveillance, Communications Surveillance, Suitability Surveillance, Employee Fraud, and other third-party data and surveillance applications, such as HR systems and physical access logs.

Holistic surveillance frees your firm from the challenges of data silos and provides a consolidated view of employee conduct risk across any number of metrics that are important to your organization.

"Metrics are driven by data," explains Steve LoGalbo, Director of Compliance Product Management for NICE Actimize. "Holistic surveillance connects the dots to give managers a 360-degree picture of risk based on summarized data from downstream systems and analytics."



2. Automation

Another challenge firms are facing is the sheer volume of alerts and communications that need to be surveilled.

As market volatility continues to cause spikes in transaction volumes, surveillance workloads are growing at a faster pace than firms can keep up with using manual processes and outdated technology.

“For many firms it’s standard practice to review random samples or conduct priority-based reviews of alerts to try and gauge misconduct,” said Mohapatra. “But trying to keep up with growing volumes of alerts with the same number of people and the same manual processes can be futile.”

Firms are solving this problem through the application of intelligent surveillance technology that can not only do a lot of the work for you, but also do it better.

If we think about the way surveillance is done today, multiple, siloed surveillance systems – suitability, trade and communications surveillance systems, HR systems, and others – are the first line of review.

These siloed systems all generate individual risk alerts and data. But to get an accurate, overall view of a regulated employee’s risk, a supervisor would need to manually collect, aggregate and review data from all of these systems, and then repeat that task all over again and again for each employee they’re managing. That would be a herculean task.

In contrast, an automated holistic surveillance solution automates the process of monitoring and supervising regulated employees and allows for risk scoring as well. It can ingest all of the inputs from different systems and produce an aggregate risk score as well as individual risk scores (based on defined misconduct areas). Serious conduct issues can be weighted more heavily in the aggregate score.

Supervisors thereby get an accurate picture of each trader’s relative risk as well as being alerted to problem behaviors much earlier on. And because the risk scoring is done entirely by the machine, there’s no inherent bias.

3. Comprehensive Coverage

Conduct surveillance is a broad area. Whether your firm is on the buy-side or sell-side, look for a solution that provides comprehensive surveillance coverage across different asset classes and regulations. Solutions like [NICE Actimize's SURVEIL-X Holistic Conduct Surveillance Suite](#) feature proven out-of-the-box risk detection models that can easily detect common buy-side and sell-side misconduct scenarios such as Insider Dealing, Ramping, Wash Trades, Large Order Entry, Marking the Open, Mark Up / Mark Down, Off Market Pricing, Spoofing, Layering, Momentum Ignition, Marking the Close, and much more.

According to Deloitte's report [Managing Conduct Risk: Addressing Drivers, Restoring Trust](#), suitability is another major area of concern for misconduct. However, the report concludes: "Poor conduct outcomes can arise when product design, marketing, sales and advice, as well as post-sale practices, are driven by concerns about 'what will sell the most' rather than what the customer needs and what is most suitable for these needs."

Advanced risk detection models can also detect suitability and best interest breaches related to a broad range of regulations and investment products, including life insurance, annuities, account rollovers, and loans on insurance policies.

For example, insurance models can determine the suitability of a life insurance policy or variable annuity based on a client's financial resources, detect spikes in replacements, surrenders or withdrawals (tied to specific advisors and accounts), and look for other tell-tale signs of risky behavior (for example when customers take out loans on long-term insurance policies to purchase other investment products).

U.S. broker-dealer firms that fall under the SEC's Regulation Best Interest (Reg BI) will also want to look for a solution that incorporates Reg BI centric models that monitor for disclosures, and analyze transaction risks, rewards and costs to determine if the broker-dealer is acting in the client's best interest. [NICE Actimize's SURVEIL-X](#) also features a 'Best Product Alternative' analytics model which highlights more suitable products the broker-dealer could have recommended based on the client's profile.

4. AI-Powered Analytics, Natural Language Understanding

Lexicon-based surveillance can zap your compliance analysts' productivity with false alerts. Natural Language Understanding (NLU) is proven to reduce false positives by 90%.

[SURVEIL-X's](#) NLU understands and analyzes communications in 45 different languages, automatically detecting people, places, products, companies, trades, assets classes and conversation topics to reveal what really happened. Fine-tuned for financial markets, it can even detect jargon indicative of market manipulation or collusive behavior.

One requirement of Reg BI is that advisors must provide timely disclosures to their retail clients. Through the combination of voice-to-text and Natural Language Processing, communication channels including voice, email, text, chat and even CRM notes can be analyzed and compared to required disclosure text to highlight gaps in proper communication.

LoGalbo explains: "When it comes to communications, conduct surveillance is especially challenging because it's unstructured content. NLP and machine learning are continuously evolving and getting more advanced and can help firms learn a lot about employees based on their communications. With NLP, we can see how people are interacting with one another, who they're interacting with and how frequently, what they're saying, how they're saying it, by extracting context and sentiment from communications. This, in turn, can surface potential issues and provide an early warning to supervisors when behaviors aren't fitting normal patterns."

"When it comes to communications, conduct surveillance is especially challenging because it's unstructured content. NLP and machine learning are continuously evolving and getting more advanced."

5. Anomaly Detection

Conduct issues can be broad and sweeping. Furthermore, a person's conduct isn't necessarily defined by one easily detectable thing they do. There are many more unknown conduct risks that firms never find out about until it's too late.

Delivering on the promise of conduct surveillance requires being able to identify subtle and connected events and patterns over time.

In their blog, [*2025 - The Future of Market Abuse Surveillance - Setting up the governance and operating model for success*](#), PwC authors explain why the future of conduct surveillance requires "moving away from 'alert factories'" to the next generation of behavioral surveillance.

Advanced anomaly detection is the centerpiece of next-generation behavioral surveillance.

Instead of focusing solely on generating alerts based on thresholds or single instances of misconduct (for example, market abuse), anomaly detection applies unsupervised machine learning to spot otherwise undetectable suspicious behavior patterns, like communications or trading activity that's outside of the norm for a specific account, portfolio manager or trader.

It does this by establishing benchmarks of normal behavior, and then comparing this behavior to new trends in data and alerts over time.

For example, is a trader suddenly sending fewer emails, perhaps in an attempt to fly under the radar? Or has a trader's daily profit increased drastically without a valid explanation? How does it compare to other traders? If a trader's P&L on a certain day is \$50,000 (compared to other traders who average \$20,000), but historically he has averaged \$45,000, that shouldn't raise an eyebrow. On the other hand, if his P&L suddenly jumps from \$50,000 to \$250,000, that could be cause for concern. Anomaly detection will automatically spot these types of risk indicators and bring them to the forefront.

Another important aspect of assessing conduct risk is having the ability to find anomalies and look at behavior comparatively and over time. This historical view also contributes to a more accurate picture of an individual's relative risk. For example, a trader who breached her credit limit one time might not be viewed as risky as one who breached it four times in the recent past.

Anomaly detection can also give supervisors a better overall grasp of a particular individual's conduct risk, whether it involves abnormal trading patterns or changes in communication habits. You can see if a trader is starting to slide down a slippery slope and maybe put that trader on heightened surveillance.

"Anomaly detection enables firms to take a more proactive surveillance approach, to get those early indicators of misconduct that could ultimately prevent worse things from happening, as opposed to traditional alerts that are merely alerting on things that have already happened," said LoGalbo.

"Again, this is nothing new," adds Cottee. "A good surveillance officer should have always sought to understand the people they monitor, and be sensitive to a person deviating from the norm. The new part is the need to automate much of this process, given increases in business volumes, alerts and available data sources, and requirements to formalize this process."

6. Self-Development Analytics

While everyone agrees that there is a need to monitor behaviors for misconduct, firms differ on their approach and definitions.

For example, with remote work environments now being the norm and an increased propensity for behavior changes, some firms might monitor employee communications for specific behaviors, like rudeness, anger and off-color remarks.

The bottom line is – when it comes to conduct surveillance, there’s no such thing as a one-size-fits-all approach. Firms need to be able to create analytical models tailored to their unique business needs.

This means you should choose a conduct surveillance solution with self-development analytics capabilities built in. By doing so, you can easily create, test and deploy your own custom analytical models. Instead of wasting time coding, and sourcing and scrubbing data, your business analysts can focus their time, energy and expertise creating models that address your firm’s most pressing conduct risk use cases.

Cottee believes this is a game-changer “You can build or modify analytics to suit your business, which is what regulators are increasingly demanding, and you’re not fighting for a place in a vendor’s development queue.”

“You can build or modify analytics to suit your business, which is what regulators are increasingly demanding, and you’re not fighting for a place in a vendor’s development queue.”



7. Robust Reporting and Data Visualization

Conduct starts at the top, both literally and figuratively.

According to Deloitte's report [*Managing Conduct Risk: Addressing Drivers, Restoring Trust*](#), both leaders and regulated employees within financial services firms need to be held to account for poor conduct, lest individuals come to the conclusion that "contraventions are acceptable and rules are bendable."

Furthermore, under SM&CR, board members and senior managers of a firm can now be held legally culpable for their own conduct and the conduct of their employees.

"Under SM&CR, every employee apart from a few exceptions, has to be aware of their own conduct and how it can affect the firm," added Cottee. "So it's up to the managers to monitor their staff, but at the same time their staff needs to be aware of their conduct as well."

But while accountability looms large, at the end of the day C-level and other executives in the management chain have few tools to visualize and understand where conduct risk really lies within their organization. Without proper insight, it's hard to have proper oversight. Too often, managers only become aware of an issue well after the fact, and the reputational damage has been done.

To streamline and strengthen accountability, firms need strong reporting engines to synthesize conduct risk data.

If your firm is addressing this reporting challenge by hiring teams of expensive data scientists it may be time to think again.

[SURVEIL-X](#) can transform data into actionable information and put it in the hands of C-level executives, using powerful visualization dashboards. Executives get 360-degree visibility into conduct issues and instantly know where the greatest risks lie, whether or not current controls are working, and where more resources need to be allocated.

The dashboards present summary level data in an intuitive, graphical, easy-to-read format, enabling executives to view business risk on a global, divisional, regional, and even employee level. Executives can see how different types of conduct risk are trending (based on numbers of alerts), and where risk is coming from (e.g. markets surveillance, communications surveillance, sales practices and suitability, etc.), and even drill down into employee risk scores to understand root causes of conduct risk both organizationally and on an employee level.

The dashboards also synthesize a firmwide-view of operational effectiveness based on global data. Executives get insight into how compliance analysts are spending their time, relative to where the highest levels of risk reside in the organization, so they can make faster, better informed decisions about reprioritizing compliance workloads or reallocating resources. It can also highlight negligence when analysts avoid investigating high risk alerts.

Because the dashboards use roles-based permissions, business level managers only see the information they need to manage their respective teams and business areas.

8. Enterprise Risk Case Management

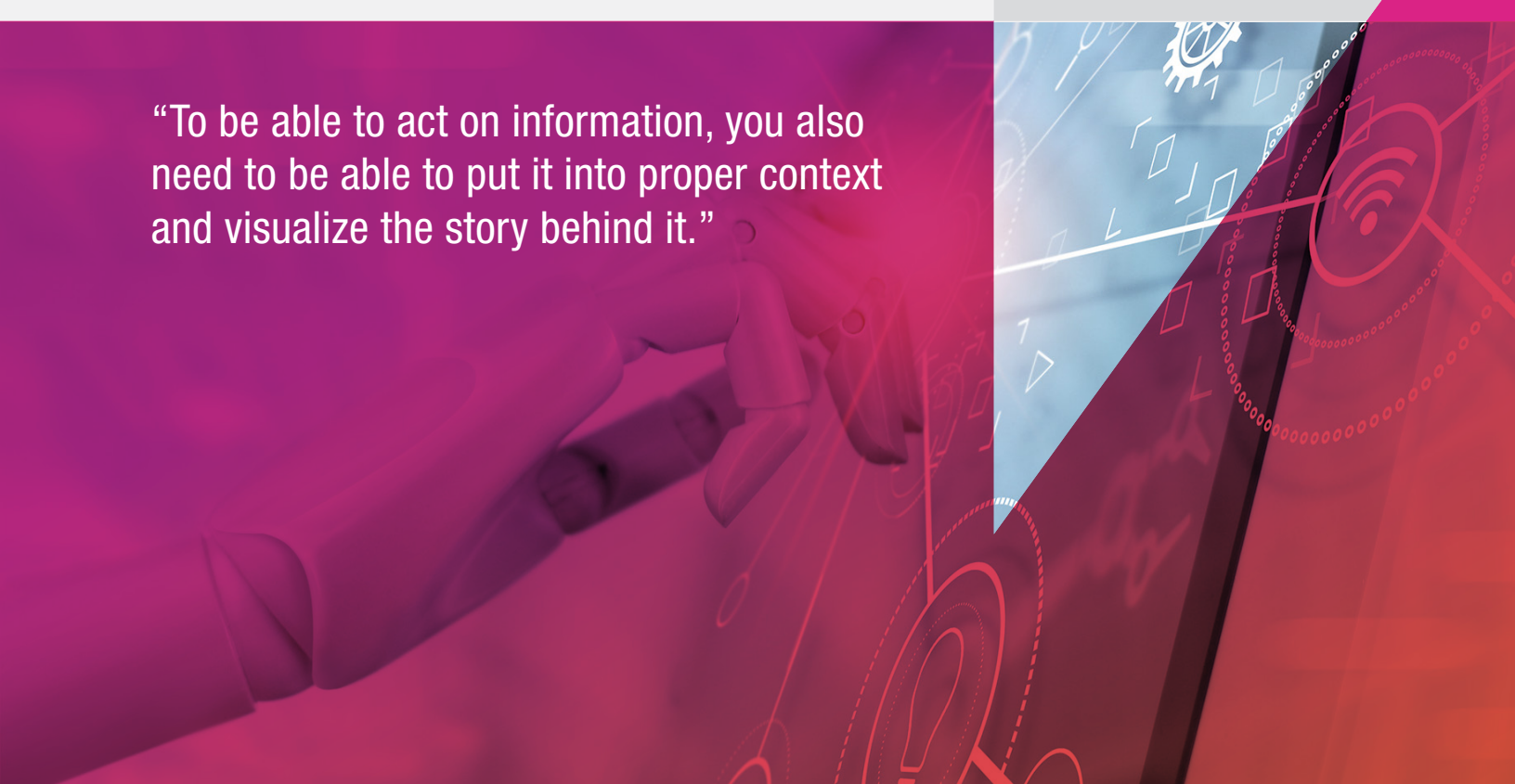
Once you discover instances of misconduct, the next question is how do you manage all the work associated with these cases?

If your firm relies on disconnected surveillance solutions to evaluate and alert to misconduct, your analysts are likely working in different case management systems too.

With [SURVEIL-X](#) analysts can do all of their work in one system, and complete investigations in record time. Let's say your firm's compliance unit supports multiple business lines and various types of alerts (e.g. Market Abuse, Sales Practices & Suitability, etc.) Now, every alert and investigation across your enterprise can be managed in one system, saving time, money and resources.

To be able to act on information, you also need to be able to put it into proper context and visualize the story behind it. With [SURVEIL-X](#) analysts are able to intuitively visualize all of the information they need to understand and evaluate risks, and quickly connect the dots, draw conclusions and make decisions. Analysts get insights into market events, trading patterns, and conversations, and can clearly see what was done and said and why, with links to related market data, news, communications, HR data, compensation information, and more.

“To be able to act on information, you also need to be able to put it into proper context and visualize the story behind it.”



9. Advanced Technology for Virtual Work Environments

Today's work-at-home environments come with their own set of conduct risk challenges.

With more regulated employees now working from home, physical oversight is not as easy, and in many cases, not even possible. Additionally, remote work environments open the door to more types of conduct risk. The ability to identify conduct risk across multiple dimensions and across the time continuum has never been more essential.

"If you're a trader working in the office, you've got compliance literally sitting next to you, monitoring what you're doing, seeing whether you're using your own personal devices, and so on," Cottee pointed out. "But when you're working from home, how can a manager actually be sure you're not bypassing the rules? Work from home opens the door for more potential conduct abuse because there's nobody looking over the trader's shoulder."

Additionally with the potential for new communication modalities (e.g. mobile phones) not being recorded, this can create gaping holes in conduct surveillance. How do you identify misconduct if a trader is using an unknown device to deliberately attempt to avert detection?

[SURVEIL-X's](#) anomaly detection addresses this. Let's say a trader used to get 20 orders a day and took 20 phone calls a day when they were in the office, but now they're getting 20 orders a day and only 5 of those related calls are being recorded. Similarly, if you had a trader who was earning \$100,000 a day in profit in the office, and is now racking up \$500,000 a day in profit working from home – anomaly detection will identify and alert to these early warning signs of conduct risk.

In today's challenging times, there's also a growing sense of frustration that can naturally spill over into the workplace. This can have a pronounced effect on the way employees communicate with each other, and with your firm's customers. Aggression, short-temperedness, instances of bullying or harassment, and other atypical behaviors can arise, and this can impact morale and customer perceptions of your brand. Through conduct surveillance, Natural Language Processing can identify problem interactions for a closer look.

"Work from home opens the door for more potential conduct abuse because there's nobody looking over the trader's shoulder."

10. Data to Link Conduct to Pay to Drive Culture

Conduct drives better culture, and having accurate, objective conduct risk data available at the regulated employee level gives financial services firms a way to drive better conduct by linking conduct to compensation. Some wholesale banks are already incorporating conduct into their performance appraisals.

In 2019, the Financial Conduct Authority (FCA) hosted Conduct Roundtables with 18 wholesale banks, each of which was represented by a group of staff at the vice president level or equivalent — termed the “Engine Room.” The roundtables culminated in the [FCA's latest report](#) titled ‘*Messages from the Engine Room*’ 5 Conduct Questions, which reflects the FCA’s findings and perspectives.

One area covered in the [report](#) is the link between conduct and pay. In the report, roundtable participants said that the conduct element of performance reviews was weighted at around 50%, and that 5% of their collective staff had received a remuneration increase of at least 10%

for good conduct, while 1.4% had their remuneration reduced by at least 10% for poor conduct. The FCA applauded the firms’ progress to date but also said there was much room for improvement.

“Compensation drives behaviors,” Cottee said. “By monitoring conduct and linking pay to conduct, firms can ethically reward people who do a good job, and at the same time, be a lot more transparent with shareholders.”

This concept also aligns with another key finding of Deloitte’s report, *Managing Conduct Risk: Addressing Drivers, Restoring Trust* which is that in order to address misconduct, firms need to build balanced scorecards for human resource decisions. The report says: “Organizations are now placing increased emphasis on an individual’s ethical, compliance and regulatory history...there has been significant focus on compensation and remuneration.”

Undoubtedly, firms need a mind shift to make further progress in this area, but the right conduct surveillance solution can certainly help.

“Compensation drives behaviors and by monitoring conduct and linking pay to conduct, firms can ethically reward people who do a good job, and at the same time, be a lot more transparent with shareholders.”

Conduct Surveillance Use Case: Raising the Bar with AI-Powered Analytics, NLP and Sentiment Detection

Company

Leading global consumer bank with 100+ million customers.

The Challenge

Scientific research indicates that the presence or absence of specific types of sentiments expressed in communications can be an indicator of increased potential for conduct risk. Understanding this, compliance executives at a leading global consumer bank decided to embark on a test case to see how they could apply advanced AI techniques to detect and classify communications containing a range of sentiments and emotions — including fear, unfairness, mistrust and aggression — that could be early indicators of conduct risk.

The executives also sought to identify hotspots of negative and positive sentiments and emotions across teams within the organization, to test whether or not managers and peers could negatively or positively influence the behavior of others with whom they frequently communicated.

The Solution

The NICE solution tested by the bank ([SURVEIL-X](#)) applied sophisticated NLP (Natural Language Processing) techniques to analyze a sample dataset of half a million email messages across 20,000 employees. As a first step in the process, NICE data scientists scrutinized the dataset to help train the data models to accurately identify different sentiments the bank wanted to test.

For example, one driver of conduct risk identified by the bank was defensive communication, defined as a tendency to attack the self-concepts of other people in order to inflict psychological pain. Examples included name calling, put-downs, sarcasm, taunting, and yelling.



To detect and accurately categorize defensive communications, the surveillance system first needs to understand what the communication is about. To determine this, [SURVEIL-X](#) uses NLP to extract who's speaking (the players), what they're talking about (the topic), and finally the intent (the sentiment/emotion) within the conversation. The system then assigns a confidence score to each detected sentiment/emotion.

Using anomaly detection, [SURVEIL-X](#) can also run an entity analysis to identify how a particular employee's sentiments or emotions are changing over time, and if negative behaviors that can potentially lead to misconduct are building.

All of the data is distilled into color coded dashboards (red for employees who predominantly express negative sentiments/emotions, blue for employees whose emotions and sentiments are mostly positive). Managers can then filter employees based on scores, and drill down into employee data to view trend timelines, behavioral spikes and contributing factors. They can even view actual underlying communications.

[SURVEIL-X](#) also applies social network analysis to construct heatmaps to identify who's communicating with whom, as well as the different emotions being expressed.

Learn More

Interested in learning more? We invite you to click on the links to additional resources below:

[SURVEIL-X Conduct - Brochure](#)

[The Future of Surveillance - eBook](#)



About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com/compliance

compliance@niceactimize.com

Copyright © 2021 NICE Actimize - All rights reserved