acuiti management intelligence

RESEARCH REPORT

Getting to the risk quicker

How trade surveillance leaders are dealing with an increasingly complex environment

IN ASSOCIATION WITH

EVENTUS

Table of Contents

Introduction

Trading technology has evolved rapidly in recent years. Electronification has spread to all asset classes and varying levels of hybrid or fully electronic execution are now in place across most markets.

At the same time, regulations governing trading have grown in scope, detail and enforcement. So has the sophistication and complexity of trading products and techniques.

These trends, along with a sustained increase in trading volumes over the past decade, have increased firms' challenges in monitoring and surveilling trading activity.

Since the 2007/8 financial crisis, regulators have promulgated specific regulations and developed expansive surveillance methods, giving them significant mandates and capability to identify and stamp out abusive activity in markets.

Enforcement of these mandates has built momentum in recent years. After its first prosecution of a high frequency trader for spoofing in 2016, US authorities have made full use of powers granted to them in the Dodd-Frank Act and other frameworks to pursue other such cases.

Subsequent prosecutions also target firms that fail to supervise effectively for spoofing within their organisations, and US enforcement agencies have also targeted non-US citizens.

While the US has outpaced other regulators in the velocity and amount of post-2008 cases it has closed, the regimes covering other leading financial jurisdictions are no less far-reaching.

Firms operating in Europe have been covered by the EU's Market Abuse Regulation since 2016, and prior to this the Market Abuse Directive since 2003. Since this time there has been an increase year-on-year in the regulatory enforcements for market manipulation and insider dealing.

A common effect of these rules has been to grow firms' operational burdens. This has necessitated a bulking up of compliance departments and surveillance tools to monitor

and capture the trade data that regulators demand.

These underlying pressures escalated in 2022. Sustained volatility across asset classes led to large increases in trade volumes, which put internal systems and compliance personnel under pressure.

This has raised questions about the capacity of surveillance analysts to maintain pace with the growing volume of surveillance data to review, and about whether legacy trade surveillance systems are capable of meeting current needs and challenges.

Manual fixes and bespoke technology builds might not be sustainable as complexity and volumes further increase in the future. The twin pressures of heightened regulatory scrutiny and increased data volumes will continue.

To understand how firms are dealing with the growing challenge and complexity of trade surveillance, Eventus commissioned Acuiti to conduct an independent research project to analyse the key challenges that face banks, brokers and proprietary trading firms when structuring effective trade surveillance operations.

For this project, Acuiti surveyed and interviewed 71 senior trade surveillance, risk, compliance, technology and trading executives to collate their views on how they are approaching both current and expected challenges in this field.

The key findings are:

- The traditional dichotomy between in house development and third-party trade surveillance systems is blurring, as new buy and build vendor platforms emerge that incorporate advantages from both models
- The complexity of complying with trade surveillance rules is increasing, with regulation considered a major driver by market participants
- Firms' appetite for automated solutions to trade surveillance has grown due to recent increases in manual workloads
- Staffing is emerging as a key challenge for compliance departments
- Adaptability is a key element to a trade surveillance system's success, as is the ability to communicate information to regulators

Growing Complexity

Trade surveillance regulation in the world's main financial jurisdictions is onerous and increasing in scope and complexity. Firms that operate across jurisdictions have to educate themselves on intricate frameworks that must consider regional differences.

In Europe, MAR is a rules-based regulation, with a defined list of problematic behaviours. In the US, a panoply of prudential regulations and exchange rules govern problematic behaviour, with the common thread of fraud linking all of them. APAC regulators tend to follow a similar approach to their European counterparts.

The scope of activity that constitutes manipulation is also broad. Firms operating in APAC, EU, UK and US markets need to be vigilant for abusive practices including spoofing, wash-trading, front-running, insider dealing and unsanctioned communications.

Regulators everywhere have highlighted that surveillance should also be calibrated to detect anomalous behaviour that might not be specifically contemplated in a rule, but nonetheless might indicate manipulative behaviour.

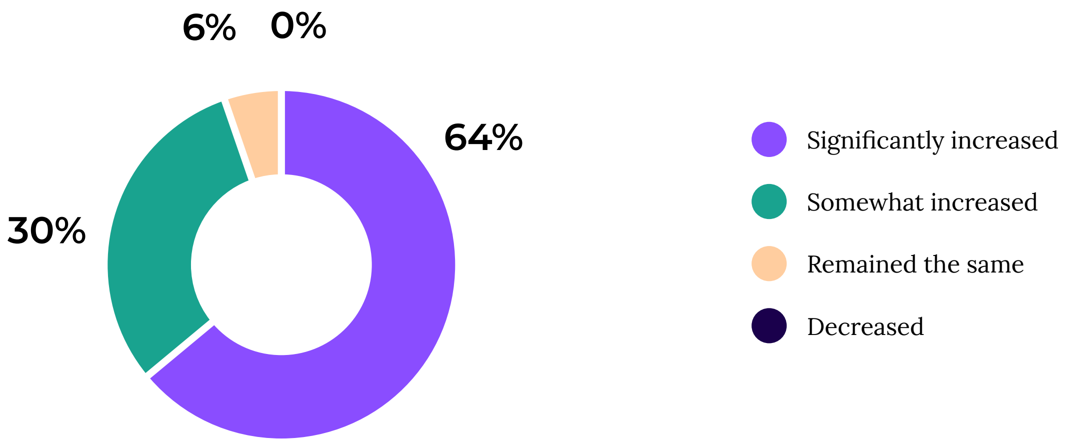
Keeping pace with market abuse and the techniques used to achieve it requires firms to have pro-active systems in place. Regulation enforces this imperative. While authorities vary in the structure of their mandates, a common feature of these regimes is the onus they put on firms to actively manage their trade surveillance.

Guidance from the Futures Industry Association for members operating under MAR is for firms to tailor alert systems to their activities, and not rely on off-the-shelf solutions.

The FCA has also impressed on firms the need for surveillance risk assessments that are comprehensive and up to date. MAR compliance requires that firms make continual situational judgements and this in turn necessitates a constant process of assessing and enhancing internal controls.

Regulators also demand that these systems produce large and detailed bundles of trade data from firms. This has presented operational challenges, not just in the quantity of information to be managed but in determining what data is relevant.

Over the past three years, how has the complexity and challenge of trade surveillance within your role changed?



In the EU, both Article 16 (6) of MiFID II and Article 16 of the MAR regime require firms to store and report trade data that could lead to a transaction, regardless of whether the transaction happens or not.

The UK is covered by similar regulation in the FCA's STOR Regime. In the US, Dodd-Frank demands that firms provide complete audit trails that can be used for "comprehensive and accurate trade reconstructions".

The breadth of these requirements has often led to uncertainty. To take one example, the UK FCA's STOR regime contains uncertainty for firms around whether only transactions that are proven to be potentially abusive should be reported, or whether anything suspicious should be submitted as an order report.

In the enforcement climate described above, areas where the path to compliance is open to interpretation create risk.

Recent evidence shows that regulators have taken an aggressive approach to non-compliance. In addition to their actions

on spoofing, US regulators' very public crackdown on big name banks' supervision of personal communications channels this year demonstrated their readiness to wield fines worth hundreds of millions of dollars if they see trade surveillance as deficient.

The overwhelming majority of participants in this study — 94% — felt that the complexity and challenge of trade surveillance within their role had increased over the past three years, with 64% saying it had significantly increased. As recent US fines have shown, not keeping on top of new developments can be costly and inflict reputational damage.

Even when market participants felt more confident that they understood regulatory requirements, the scope of trade data that they needed to capture presented its own operational challenges. These challenges are felt not only by compliance analysts, but also by trading, execution and brokerage desks that must regularly collect and process huge amounts of data. Sustained volatility this year has augmented this — causing spikes in volumes and with that, the number of trades alerts that require further investigation.

While sell-side firms' technological capacities have sometimes struggled to keep pace with regulatory demands for trade surveillance, trading desks have improved their ability to capture trade data as they increased the electronification of their offerings and trade activity.

As firms' ability to capture a broad and detailed range of data has increased, regulators continue to push for improved oversight of markets. Authorities expect firms to invest in building those appropriate data-capture capabilities.

The regulatory state of play

US authorities have been active in enforcing cases of market manipulation, like spoofing. Supervising for market abuse is the responsibility of different federal authorities, which have oversight for different asset classes, most notably the CFTC and SEC. As spoofing is a criminal act under Dodd-Frank, the Department of Justice has also been a prominent enforcer of the rules.

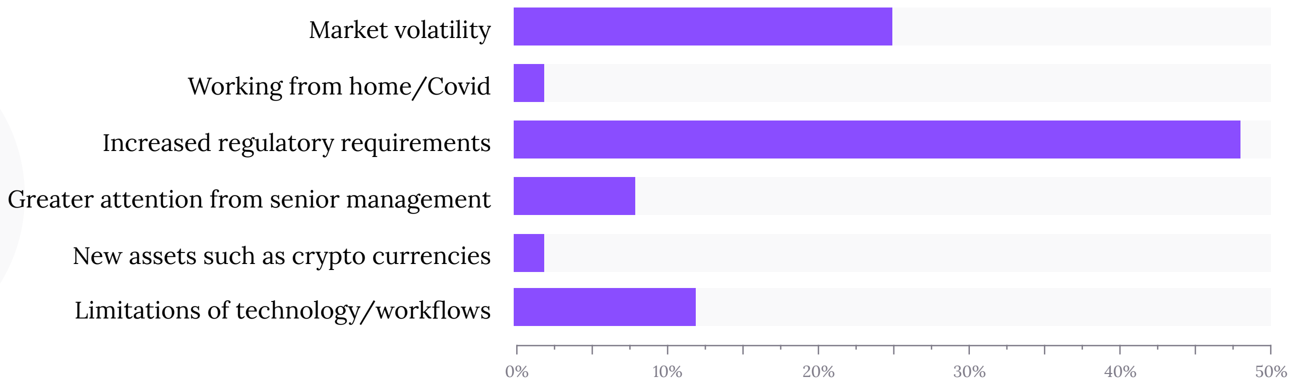
Authorities operate under a goals-based approach to regulation, with enforcement covered by a variety of different regulations. In the EU, the Market Abuse Regulation is enforced by national competent authorities, such as BaFIN in Germany or the AMF in France. The UK, which lifted MAR into its own legislation after Brexit, gives these responsibilities to the FCA. MAR is a rules-based framework and emphasises the importance of a systematic approach to trade surveillance that incorporates regular assessment.

In APAC, regulatory regimes are fragmented by country. However, similarities with other frameworks are evident. MAS has emphasised the importance of periodic reviews and structural processes in ensuring well-functioning trade surveillance systems, for example.

Assessing the challenges

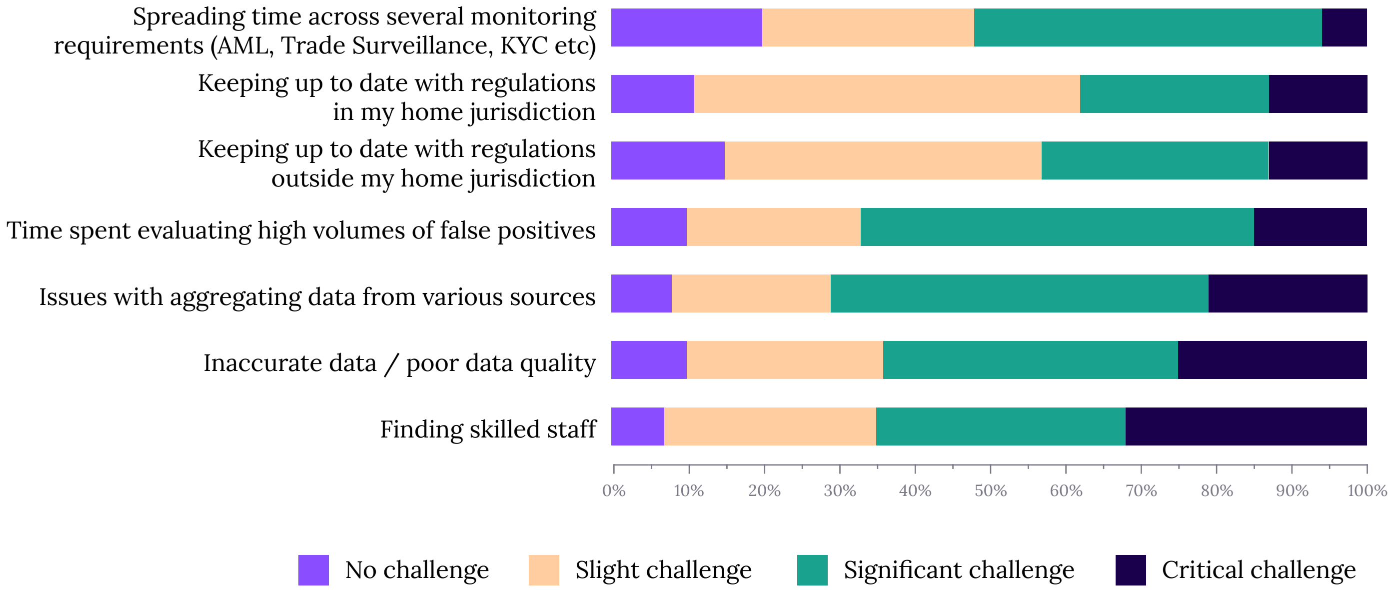
When considering the drivers of increased complexity in trade surveillance, respondents cited increased regulatory requirements as the main factor by some distance (48%). This was followed by market volatility and limitations of technology. The challenge posed by Covid-19 has significantly receded though, as firms return to normal working practices.

What factor has had the biggest impact on that increase?



However, there is a growing skills shortage to contend with. Compliance and surveillance teams are increasingly finding themselves spread too thinly to handle the quantity of alerts coming in and often struggling to retain talent.

How much of a challenge do the following factors pose to your day-to-day surveillance operations?



The survey highlighted that among the greatest challenges for day-to-day surveillance, finding skilled staff has been the biggest — 32% identified it as a critical challenge and 33% as a significant challenge.

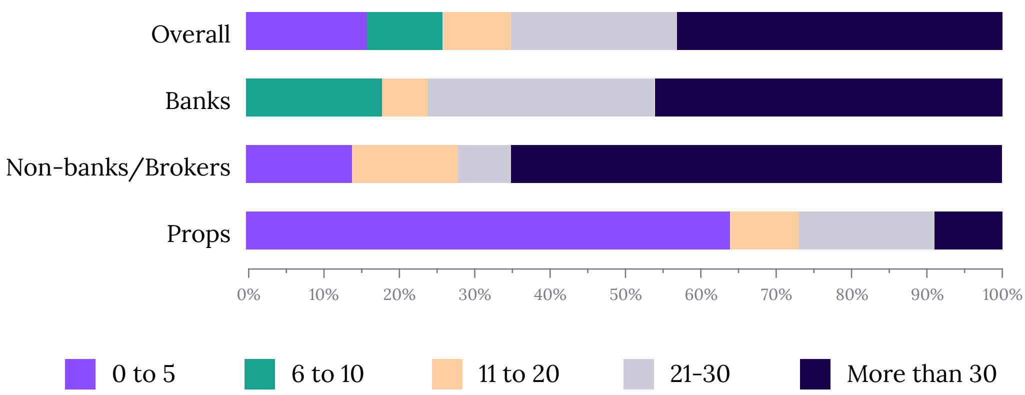
This was a particularly acute problem for banks in the UK, 68% of which cited this as a critical challenge (see box-out – regional challenges).

Interviews for this study showed that, when firms do find talented compliance analysts, they then often face a struggle to keep them, with intense competition from rivals for staff.

The shortage of talent is exacerbated by the manual nature of investigating and closing alerts.

Despite technological advances in other areas of the sell-side, trade surveillance still relies heavily on manual review, which is neither rewarding nor efficient. Almost half of executives that took part in the survey reported that analysts were spending more than 30 hours a week manually investigating and closing alerts.

On average, how many hours per week does a trade surveillance analyst at your firm spend manually investigating and closing alerts?



This trend was clearest among banks and brokers, where 45% and 64% of respondents respectively said that analysts at their firms were spending over 30 hours a week manually investigating and closing alerts. Proprietary trading firms reported greater efficiency, with 64% spending 0 to 5 hours a week on such tasks.

Prop traders' efficiency in processing the volume of trades that they deal with daily was attributed to overall lower volumes, a lack of client flow and the greater automation of their trading environments.

Despite this, 36% of prop shops reported an increased level of manual input over the last 18 months (the rest saying it had remained the same). For banks and brokers this increase was even more pronounced – 70% of banks and 57% of non-bank FCMs and brokers said levels of manual intervention had increased during this period.

In interviews, executives reinforced the frustration felt by banks and brokers over the time spent manually analysing alerts. This burden has been exacerbated by high staff turnover.

In one multinational bank, a senior compliance analyst said that his team had found it very hard to keep staffing at optimum levels due to analysts leaving during the Covid-19 pandemic and not being replaced fast enough. This led to a higher burden for those that remained.

For multinational banks, or any sell-side firm with cross-border operations, higher manual input brings other stresses aside from inefficiency and staff burnout.

Many banks have offshored surveillance roles to Asia, including locations like Manila. In some of these jurisdictions, labour laws can restrict overtime or make it significantly more expensive.

An additional complication in multinational surveillance systems is time differences, which have created challenges for closing cases within deadlines. In this context, executives are looking to automate processes to free up staff, so that they can focus on more value-additive processes.

From senior management to compliance staff closer to day-to-day surveillance, respondents were clear that automating certain parts of the surveillance process could bring sufficient efficiencies to operations. This would then allow compliance analysts to focus on higher level investigations.

Senior executives highlighted a readiness to invest in better technology and more advanced solutions such as robotic process automation and machine learning, if the technology could deliver efficiencies.

Regional variations

An analysis of the survey data by region reveals some notable local trends in the surveillance challenges faced by firms.

North America was the region in which firms reported that the complexity of trade surveillance had increased the most over the past three years — 74% reported a significant increase in complexity compared with 56% in the EU and 67% in Asia.

The factors driving the increase were broadly similar across regions, with increased regulatory attention the top factor followed by market volatility. However, firms based in Asia were more likely to report greater attention from senior management as a factor that had increased the challenge of surveillance. North American firms were more likely to say that limitations of technology and workflows was a key factor.

This finding is reinforced by the fact that North American firms were significantly more likely to report critical challenges with their surveillance technology when it came to reliance on third-parties to amend or add procedures and the inability to add or amend procedures quickly.

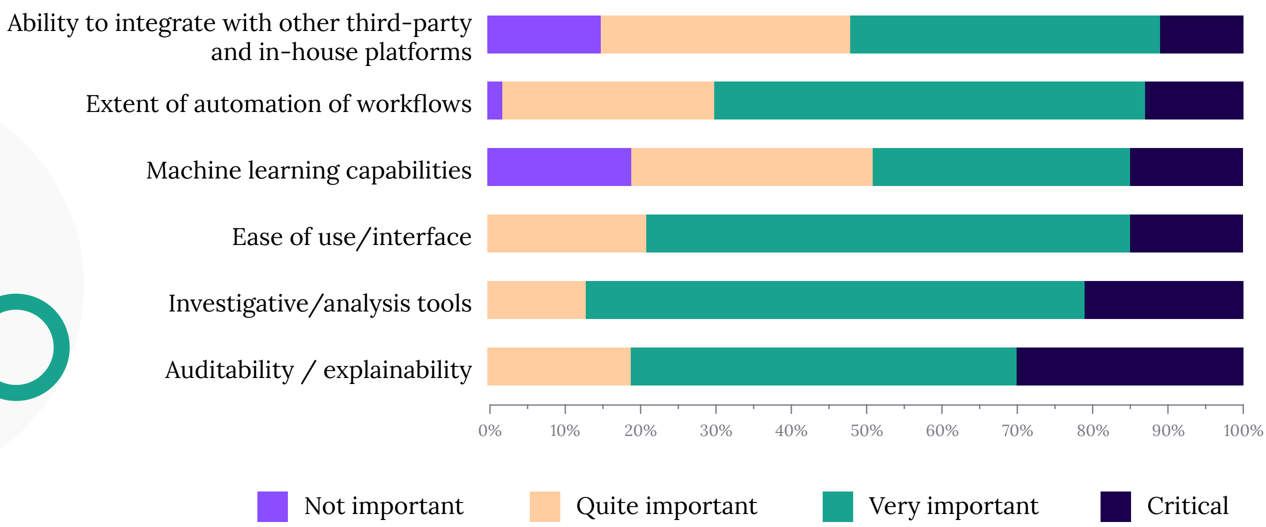
For the challenges faced in day-to-day surveillance operations, there were significant regional differences. Firms in Europe, and in particular in the UK, were much more likely to report difficulties in finding skilled staff as a critical challenge.

US firms were twice as likely to cite critical data challenges, both in terms of inaccurate data and with issues aggregating data. Asia-based firms were most likely to report critical challenges in terms of keeping up to date with regulatory change.

Finding the right platform

As part of this study, Acuiti asked senior executives what they considered the most important elements of a successful trade surveillance system.

How important are the following functions when considering the adequacy of your trade surveillance platform?



The most critical factor to get right was auditability and explainability — 51% said this was very important and 30% said it was critical.

Investigative and analysis tools were very important to 66% of respondents and critical to 21%. For more complicated instances of malpractice, such as certain insider trading cases, these capabilities are particularly important.

While machine learning infrastructure ranked less high in importance, there was a bifurcation in the market. While 20% said ML was not important, for 48% it was either very important or critical. This percentage rose to 64% of banks (compared with just 27% of proprietary trading firms).

There is also a clear desire for more automated workflows, something that 57% considered very important and 13% critical. Greater efficiency in this regard would help with the staffing constraints that this report has detailed.

Good product assistance was also flagged as a key factor and an often-underappreciated element for firms when considering trade surveillance systems.

Most firms will focus on enhancing technological sophistication, but quality support staff also play a crucial role. This doesn't just apply to resolving technological difficulties, but also to ensuring flexibility in keeping on top of regulatory developments and nuances, which some providers now include in their offerings.

The ability to integrate with other platforms used by the firm, whether developed inhouse or purchased from a third-party, was considered very important by 41% of respondents (33% considered it quite important and 11% critical).

For smaller development teams in particular, normalising messaging and trade reference data between different platforms across the trade cycle can be particularly time consuming.

What are main drivers your firm identified in selecting a third-party trade surveillance platform?

1	Need to surveil across multiple asset classes and product types
2	Market coverage
3	Track record/reputation in the market
4	Ease of configuration and workflow functionality to make changes on-demand
5	Need to conduct surveillance of more asset classes and products
6	Cloud solution for ease of integration and scalability
7	Increase available time for compliance team to handle tasks
8	Buy vs build analysis
9	Regulatory fines driving to adopt the latest and/or new platforms

Once you've decided on adopting a trade surveillance solution, what are your main considerations when evaluating which to choose?

1. Cost efficiency
2. Analytics
3. Intuitive user interface
4. Workflow automation
5. Fast implementation
6. Reporting capabilities
7. Integrations with existing systems
8. Self-serve customisation of rules and alert thresholds
9. Operates across multiple business units
10. Scalability

When selecting a new system to onboard, the most important factor for respondents was optimising the total cost of ownership, with 34% (the largest proportion) of respondents saying this was their main motivation. Analytics capabilities were highly important too, with 32% of respondents citing this as their main driver when selecting a system.

In house vs buy and build

Before structuring a trade surveillance system, market participants' first decision is whether to develop in-house or buy from a third-party vendor.

Both have their pros and cons. For those seeking to minimise regulatory risk, third-party systems have a clear advantage. Interviewees reported that regulators regularly express a preference for vendor systems owing to their familiarity with the platforms.

In-house development still has a strong pull for those that can afford it though. Those who chose this route mostly did so because it allowed them to maintain full control over the build and infrastructure.

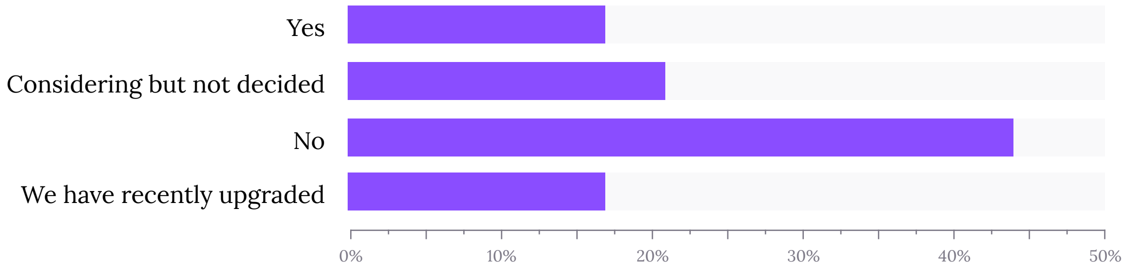
Cost-efficiency was the second most cited reason. Given the high fixed costs of hiring the right developers and harnessing the best technology, as well as the potential for overrunning costs, this may not seem intuitive. But as with other in-house technology projects, the total cost of ownership is often not worn by the function or desk, whereas the cost of a third-party system often is.

However, in-house development is a route that can drain time and resources as well as potentially creating risk. This makes it non-viable for smaller firms, where the total cost of ownership will be felt more directly, regardless of which department uses the system.

This binary choice between building in-house or outsourcing has become less clear cut with the recent advances of vendors offering buy-and-build models. These allow clients to buy a surveillance platform and then customise it to their needs without consuming huge amounts of internal resources.

Buy-and-build also serves as a double tick on regulation, both in regulators' preference for third-party systems but also in providing firms with the tools to adapt systems nimbly, and in-line with their own insights on market conditions — a key principle of much of the post-2008 market abuse regulations.

Are you planning to change or upgrade your trade surveillance system(s) within the next 12-18 months?



On the operational side, buy-and-build solutions also offer firms the ability to tap into efficiencies such as automation of machine learning technologies with less lead time than in-house development.

In contrast to off-the-shelf third-party products, this technology can then be better tailored to an individual firms' own operations.

A complaint with off-the-shelf machine learning solutions in the surveillance market has been their lack of applicability to firms' actual needs. The customisation inherent in buy-and-build is one route to more effectively harnessing these technological developments.

The survey found that over half of firms had recently invested or were considering doing so. Unsurprisingly considering the recent fines, banks were most likely to be investing — a third were planning to change or upgrade their systems in the next 12-18 months.

This need for investment comes at a time when vendors have developed systems that are capable of much greater adaptability than firms have been used to with legacy trade surveillance platforms.

Conclusion

Legacy systems and processes are struggling to keep pace with increasingly complex and demanding regulation. This has only been exacerbated by the sustained volatility of this year. As these trends strengthen, compliance teams' capacity to keep up with developments is set to be stretched further.

While this would be a challenge for fully functioning departments, a shortage of skilled staff in certain jurisdictions is adding a new level of pressure to firms' operations. Those analysts that remain are often finding themselves bogged down in mundane and high-volume work that could be alleviated by automation.

Investment in automation can significantly relieve pressures on overworked analysts, allowing them to focus on more value additive investigations and processes. Competitive alternatives to legacy systems are driving innovation in the sector and greatly increasing the number of tasks that technology can handle, leveraging machine learning and other emerging technologies and processes.

These developments are coming alongside a significant evolution in the flexibility of third-party, buy-and-build systems offering a level of customisation that captures advantages traditionally associated with in-house development.

These new vendor solutions create the flexibility that firms need to adapt to changes in market conditions that could affect the character of malpractice — a key principle of modern-day market abuse regulation. This has increased the diversity of solutions at a time when much of the industry is planning for investment in surveillance software.

acuiti management intelligence

0203 998 9190
acuiti.io
info@acuiti.io

Copyright © 2022 Acuiti. All rights reserved.