SteelEye

The state of

Financial Services Compliance

2025

→ Annual Compliance Health Check Report

Contents

Executive Summary

SteelEye's Annual Compliance Health Check Report surveys the views and experiences from across the global compliance industry to provide comprehensive insights into the issues and trends shaping today's compliance functions. This 2025 report reveals a compliance landscape under mounting pressure, but also on the cusp of transformation.

Firms continue to face challenges across surveillance, data governance, and regulatory interpretation, yet most are responding with increased investment, smarter systems, and stronger internal alignment.

This year's results point to three key trends shaping the future of compliance:

Compliance budgets are increasing:
Over three-quarters of firms increased compliance spend in 2024, with many citing technology and talent as key drivers.

Surveillance is evolving:
Firms are expanding their monitoring capabilities across communications and trading channels, with a marked rise in AI adoption and voice data integration.

Confidence in surveillance coverage is growing:
An encouraging number of firms are 'mostly' or 'completely' confident their surveillance systems are surveilling all of their business records, but challenges remain in proving effectiveness and navigating near-constant regulatory change.

The current global economic climate, characterised by uncertainty and volatility, presents unique challenges for financial services compliance. Economic downturns and geopolitical instability can exert considerable pressure on financial institutions, potentially creating incentives for riskier behaviour as firms strive to maintain profit levels.

As enforcement expectations rise and regulators take a harder stance on accountability, compliance teams are being asked to do more and must stretch limited resources across an increasing array of channels and responsibilities. Many firms are responding by boosting budgets, implementing smarter systems, and strengthening internal alignment to cope with these pressures.

Success in this environment will depend on firms' ability to consolidate systems, reduce manual workloads, and demonstrate clear, data-driven oversight of compliance activities.

Despite the challenges, this year's survey results tell a story of resilience and renewal. Compliance teams are increasingly ready to meet emerging risks head-on, signaling optimism and preparedness for the future.

Compliance Challenges in 2025
Overview

Compliance teams continue to face pressure from all sides - regulatory, operational, and organisational. When asked to identify the biggest challenges in meeting their regulatory obligations, firms pointed to a mix of strategic and tactical barriers, from using management information effectively and staying abreast of regulatory change to staff resourcing.

These challenges reflect a compliance function under strain, with increasing responsibilities but often limited resources, despite an increase in budgets. Importantly, the wide range of responses also highlights that there is no single pain point - compliance leaders are managing multiple, complex demands simultaneously.

The firms best positioned to overcome these challenges will be those able to unify their data, automate routine tasks, and ensure their teams have both the tools and insight needed to demonstrate proactive risk management.

This chapter examines the report findings relating to the key challenges faced by global compliance teams

KEY FINDINGS

29% of firms struggle with using Management Information (MI) effectively to demonstrate compliance risk to the business

24% of firms flagged the huge volume of trading activity as their key concern related to Market Manipulation

15% of UK firms felt they had no major compliance challenges, an optimism not shared globally

21% of firms were also concerned about the high number of false positives in trading alerts impacting their ability to manage risk effectively

COMPLIANCE CHALLENGES IN 2025

Varied Strategic & Tactical Challenges

The most common challenge identified by respondents was using Management Information (MI) effectively to demonstrate the compliance risk to the business.

This was cited by 29% of respondents overall and featured particularly highly among APAC based firms. This was closely followed by difficulties managing control risks, staying abreast of regulatory changes, staff resourcing and addressing market abuse and manipulation.

Other high-ranking issues included consolidating and normalising structured and unstructured data from multiple sources, the ongoing complexity of monitoring electronic communications across platforms, and managing and extracting data in a timely manner.

What are the biggest challenges you currently face in meeting your regulatory obligations, if anything? (Select up to 3)

*Percentages do not add up to 100% due to multiple responses

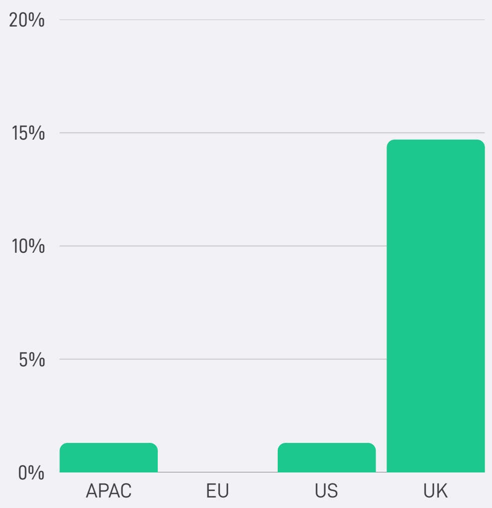
Regionally, Dutch and Australian firms reported the highest concern with staff resourcing (48% and 44% respectively). European firms cited the greatest challenge as keeping abreast of regulatory change and managing control risks in the business.

Retail Brokers showed a particularly high concern with internal control risks (70%), while Hedge Funds and Mutual Funds were especially affected by MI reporting (60% and 63% respectively).

High confidence in regulatory compliance capability among UK firms

The UK was the region by far the most confident in their regulatory compliance, with an impressive 15% of firms believing they didn't currently have any challenges in meeting regulatory obligations. This confidence was not shared in other regions, with only 1% of US and APAC firms and 0% of EU respondents believing they had no current concerns in meeting regulatory requirements.

Currently not facing any challenges in meeting regulatory obligations



These differences highlight that while many compliance teams face similar structural challenges, the intensity and type of pressure varies depending on their operating environment, regulatory jurisdiction, and organisational model.

This underlines the need for tailored compliance strategies, particularly for firms expanding into new regions or asset classes.

"The business often has challenges seeing the value-add and must be continuously sold on the often unobserved and unrealised possibility of a compliance issue."

– Chief Compliance Officer at a Global Asset Management Firm

Market Manipulation & Risk Monitoring

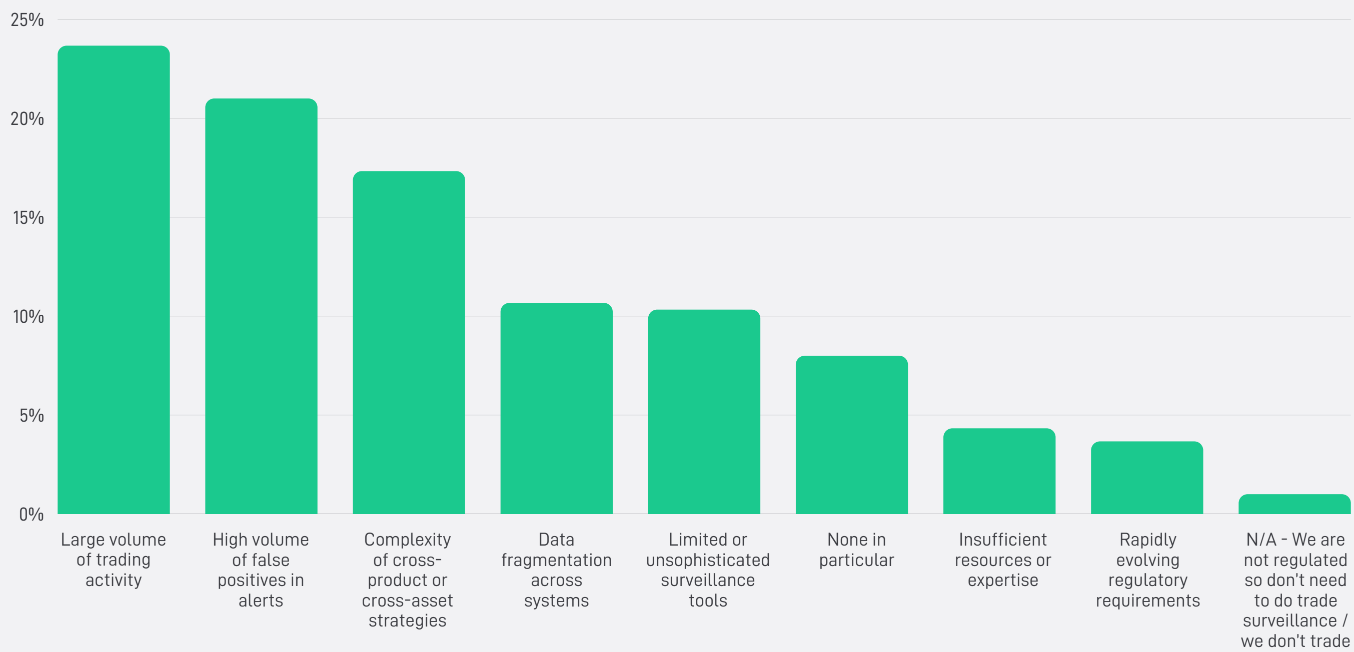
Market abuse continues to be one of the most complex challenges facing compliance teams.

Firms highlighted a range of issues that hinder their ability to detect and manage market manipulation such as spoofing, layering and insider trading.

The huge volume of trading activity was cited as posing the greatest challenge overall, with 24% flagging this as their biggest concern. This was followed by the high volume of false positives in alerts, seen as a major challenge by 21% of firms globally. This highlights the overwhelming proliferation of data that compliance teams are expected to cover, with existing systems struggling under the heavy load.

Other key issues identified were the complexity of cross-product or cross-asset strategies (17%), fragmented data sources across systems (11%) and inadequate or outdated detection tools (10%).

What, if anything, is the biggest challenge your organisation faces in identifying market manipulation like spoofing, layering and insider trading?



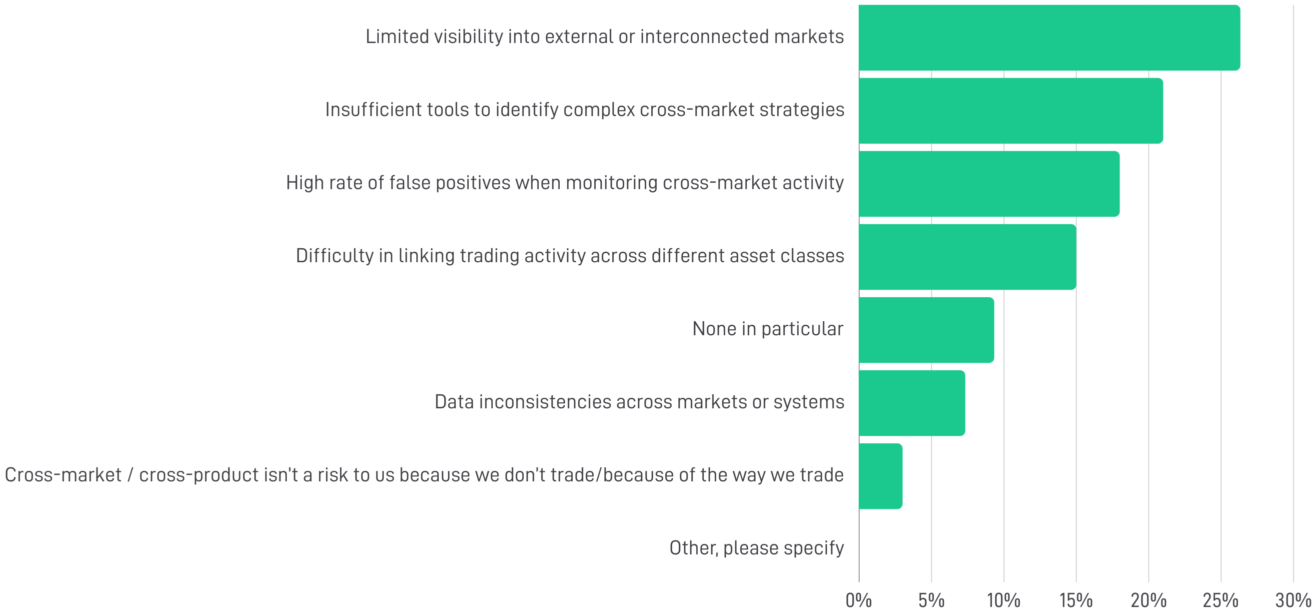
Cross-Market & Cross-Product Manipulation

When asked about their biggest challenges in identifying cross-market or cross-product manipulation, respondents pointed to difficulties linking activity across different markets due to limited visibility into external interconnected markets and insufficient tools to identify complex cross-market strategies.

These findings reinforce the need for more sophisticated and integrated surveillance solutions. Firms operating in multiple markets or handling a variety of asset types must be able to identify emerging patterns across channels, something that is only achievable with well-calibrated, integrated tools and strong data governance.

As regulators sharpen their focus on manipulative trading practices, firms that proactively enhance their monitoring capabilities will be better equipped to mitigate enforcement risk and protect market integrity.

What, if anything, is the biggest challenge your organisation faces in detecting and managing the risk of cross-market or cross-product manipulation?



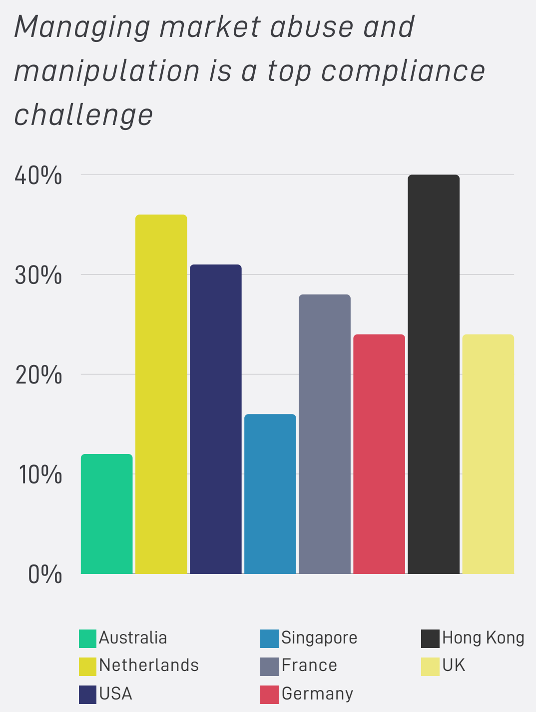
Market Abuse Detection – a Global Concern?

While firms continue to struggle with detecting market abuse, the level of concern varies significantly across regions.

Hong Kong firms reported the highest levels of concern, with 40% citing market abuse and manipulation as a key compliance challenge. The Netherlands followed closely at 36%, while France (28%), Germany (24%) and UK (24%) showed moderate concern.

In contrast, only 12% of Australian firms selected this as a top challenge, possibly reflecting differing enforcement intensity or trading volumes in their markets.

These insights suggest that while market manipulation remains a universal concern, its perceived severity is influenced by both regulatory scrutiny and market dynamics. Firms in high-alert jurisdictions may be further along in strengthening detection capabilities, or feeling more acute pressure to do so.



Surveillance Investment & Resourcing
Overview

Compliance spending is on the rise across the financial industry. Survey results show significant budget increases in 2024 driven by investments in technology and talent, reflecting mounting regulatory expectations and a need for greater capacity.

This chapter digs into the compliance team budget and the biggest trends in investment and resourcing

KEY FINDINGS

77% of firms reported compliance spend had increased over 2024

50% of respondents reported the top driver for the increase was investment in technology to support compliance processes

42% of firms were focused on investments in their data storage and archiving capabilities

68% of firms have already implemented some AI into their compliance processes, and 25% are in the process of doing so

96% of firms using AI reported improvements in their compliance processes

27% of firms reported a significant portion of compliance staff (20-40%) are working on administrative or repetitive tasks

SURVEILLANCE INVESTMENT & RESOURCING

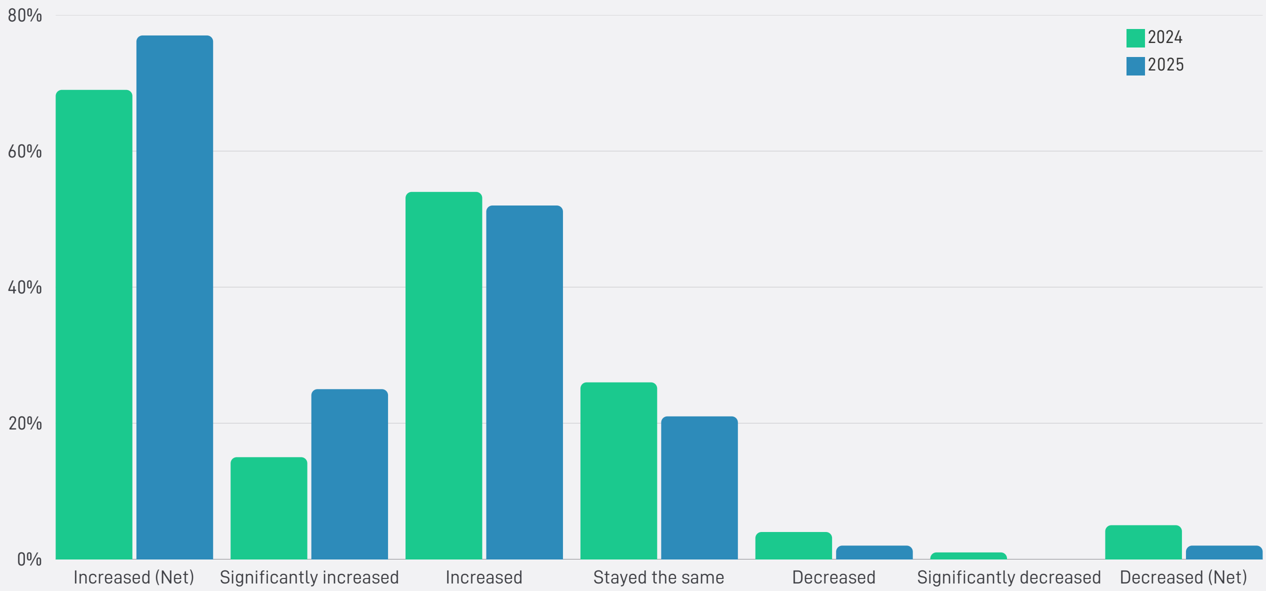
Compliance Budgets on the Rise

Compliance expenditure continues to rise across the industry. 77% of firms reported that their compliance spend had increased over 2024, with 25% describing that increase as significant.

This marks an uptick from the start of 2024, when only 69% reported any increase, and fewer firms reported large-scale investment gains.

Only 2% of firms reported a decrease in spend this year, while 21% maintained their budgets at previous levels. The continued upward trend reflects mounting regulatory expectations and a need for improved systems and staff capacity.

How has your firm's compliance expenditure changed over the last year?



SURVEILLANCE INVESTMENT & RESOURCING

Top Drivers of Budget Increases

Among firms that increased expenditure, the top drivers were:

50% **Technology to support compliance processes**

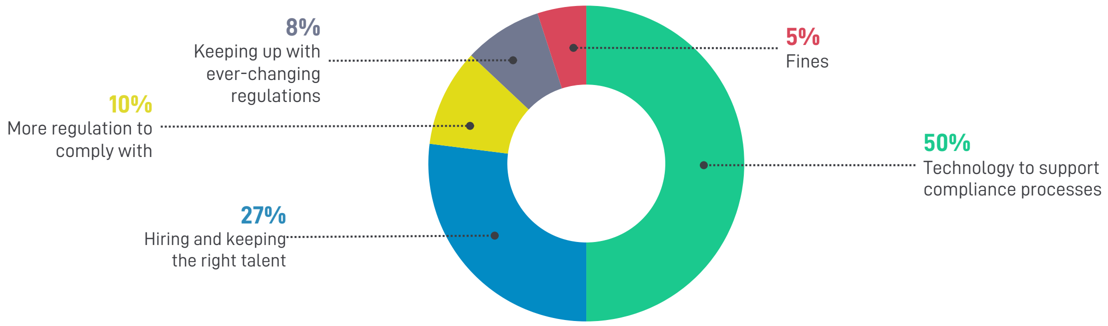
27% **Hiring and retaining talent**

18% **More regulation and faster pace of change**

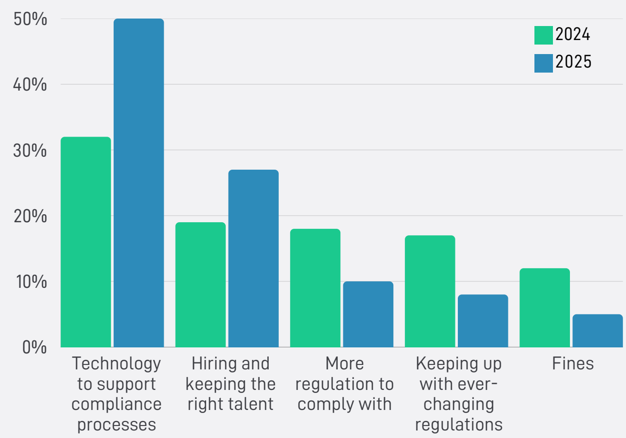
While technology remains a major cost driver, the data suggests that many firms are investing to keep up, not necessarily get ahead. This is compounded by the fact that a significant portion of compliance teams are still spending time on manual, repetitive tasks, further limiting productivity and driving up resourcing needs.

As compliance becomes more complex and cross-functional, many firms are also facing pressure to demonstrate return on investment. Strategic spend, focused on automation, analytics, and system integration, will be critical in determining which compliance functions scale effectively in the years ahead.

As you said that your firm's compliance expenditure has increased in the last year, in your opinion, what do you think is the main factor driving up these compliance costs?



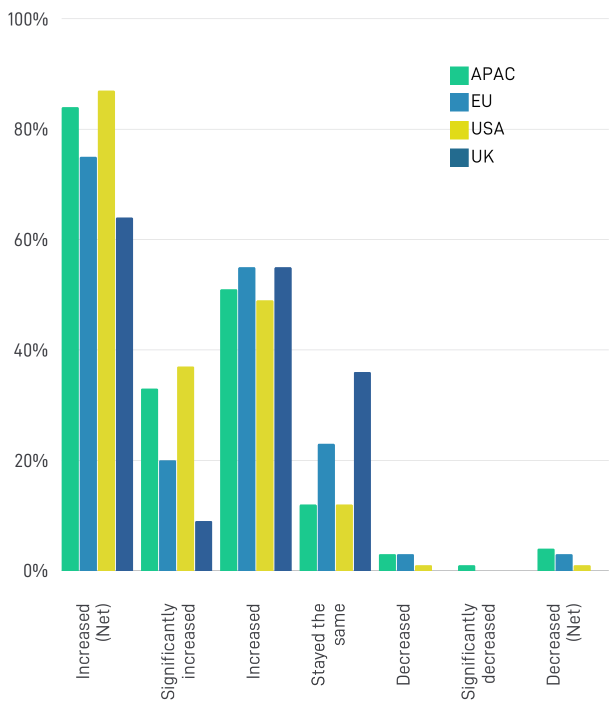
In comparison to the 2024 data, the number of firms attributing increased expenditure to both hiring and retaining the right talent, and investment in technology to support compliance processes has increased significantly. Conversely, the number of respondents citing fines and regulation as the primary factor driving compliance costs has decreased.



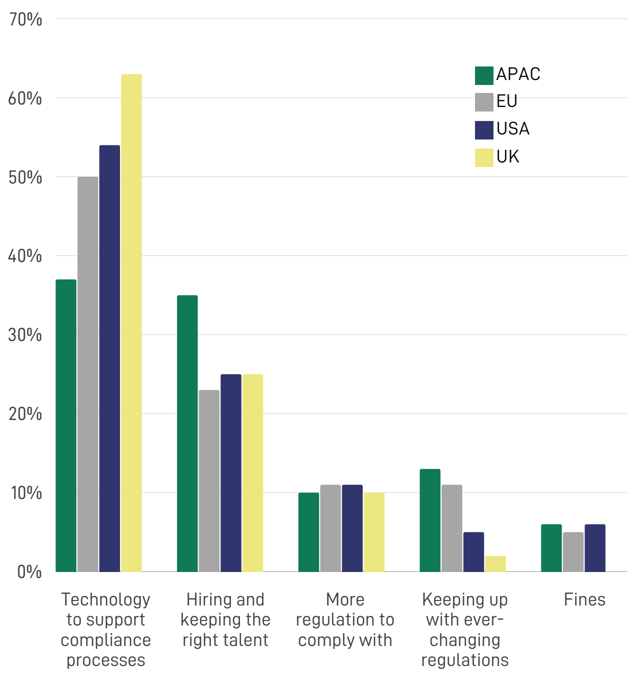
Differing spend across regions

The UK had the second lowest spend increase of all regions after the Netherlands. This could perhaps be a result of the UKs high levels of confidence in their ability to meet regulatory obligations. However, a larger proportion of UK spend increase was on compliance technology (63%) suggesting firms are continuing to invest in systems to ensure they have the right tools to keep up with an ever-evolving landscape.

Expenditure levels by firm location



Areas of spend by firm location



APAC had the highest expenditure of all regions on hiring and keeping the right talent (35%), with a significantly lower focus on technology spend (37%) when compared to other regions.

In general, the larger the firm, the greater the percentage spend on compliance technology, while smaller firms are more focused on hiring spend.

These patterns suggest a continued strategic commitment to compliance infrastructure, but also highlight the varied pressures and priorities depending on firm scale and regulatory environment.

SURVEILLANCE INVESTMENT & RESOURCING

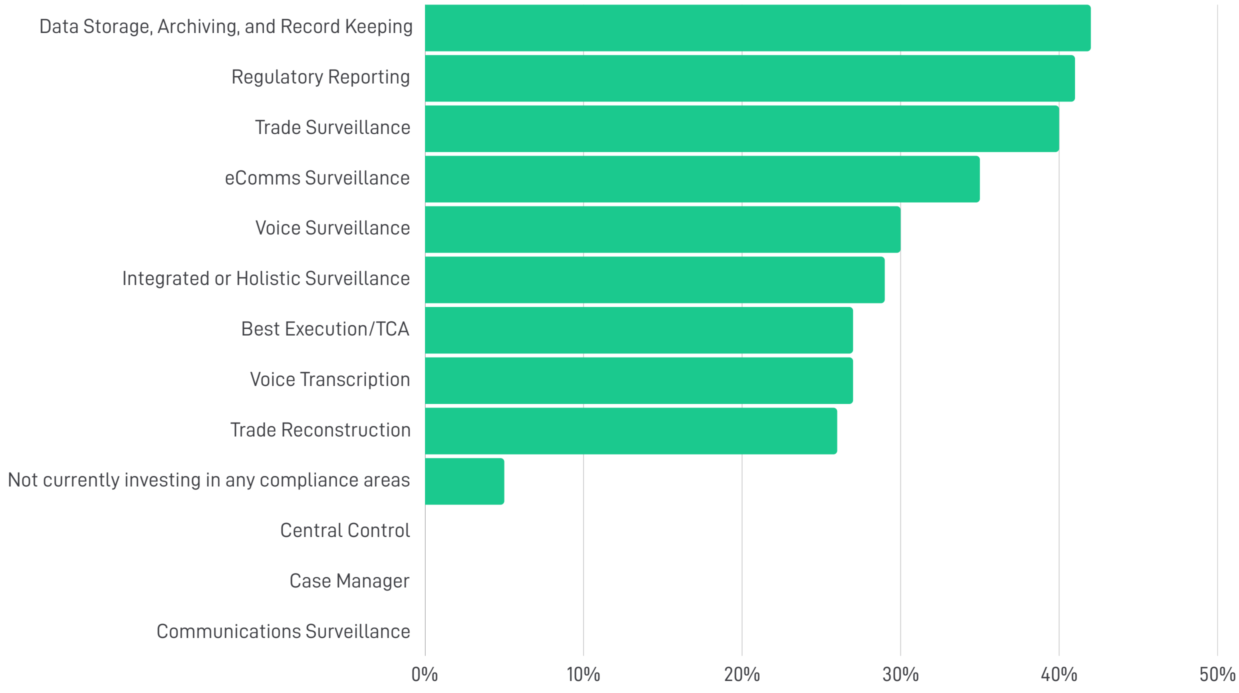
Key Areas of Investment

As regulatory scrutiny around communications and trade surveillance intensifies, firms are prioritising investment in monitoring tools that can help them demonstrate compliance effectively and consistently.

The top areas of investment for 2025 include data storage and archiving (selected by 42% of firms), regulatory reporting (41%), and trade surveillance (40%).

Communications surveillance, voice surveillance and integrated/holistic surveillance follow closely, reflecting an industry shift toward more comprehensive oversight of both structured and unstructured data.

What areas are your firm investing in from a compliance perspective, if any? (select all that apply)



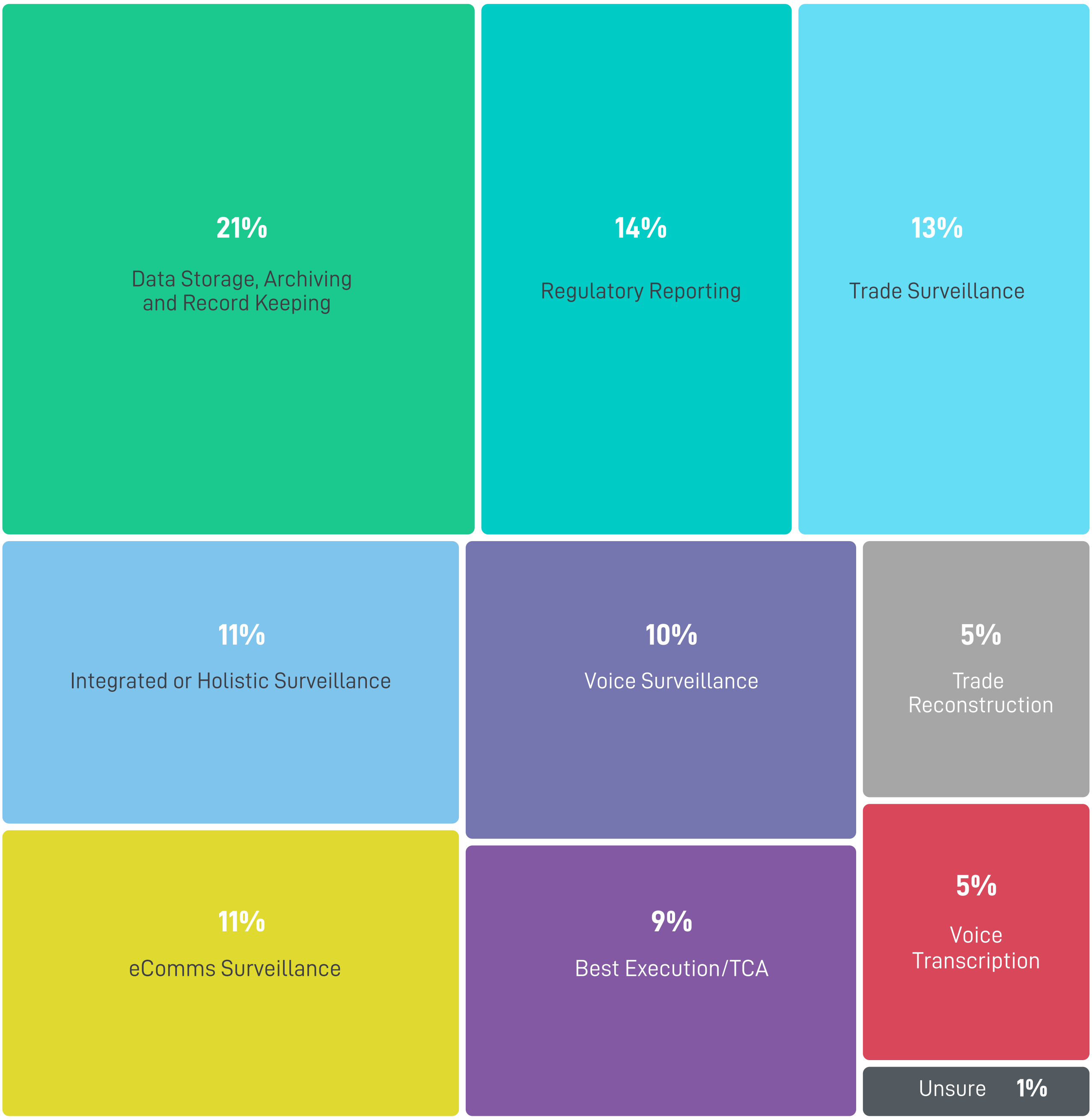
*Percentages do not add up to 100% due to multiple responses

“More channels being monitored means more demands on data storage, making it a key investment priority”

– Chief Compliance Officer at a Global Asset Management Firm

When asked to name their single highest investment priority, data storage, archiving and record keeping was by far the top priority, selected by 21% of firms. Regulatory reporting and trade surveillance followed with 14% and 13% respectively, and 11% selected both integrated/holistic surveillance and eComms surveillance.

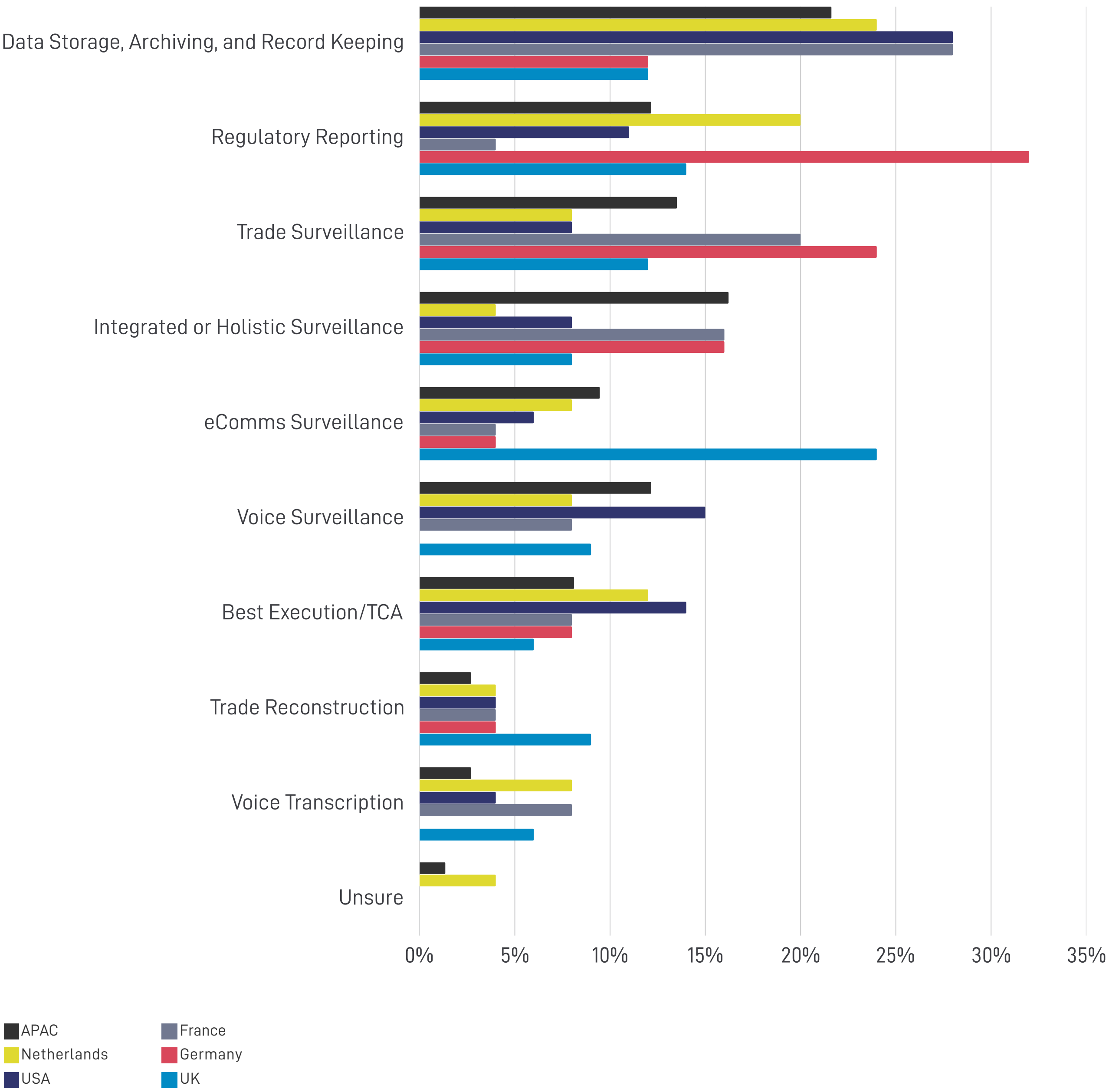
Highest investment priority areas



Geographically, Germany stands out with the highest focus on regulatory reporting, trade surveillance, and trade reconstruction, with 80%, 64% and 52% respectively of firms citing these as key investment areas. When asked to select their top investment priority area, 32% of German firms said Regulatory Reporting, and 24% Trade Surveillance. These findings could be the result of a complex and more conservative regulatory environment.

These results signal that firms are not only expanding surveillance coverage but are also focusing on foundational infrastructure. The ability to retrieve, interpret, and present surveillance data is increasingly seen as essential, especially as regulators demand more robust and timely reporting.

Highest investment priority areas by location

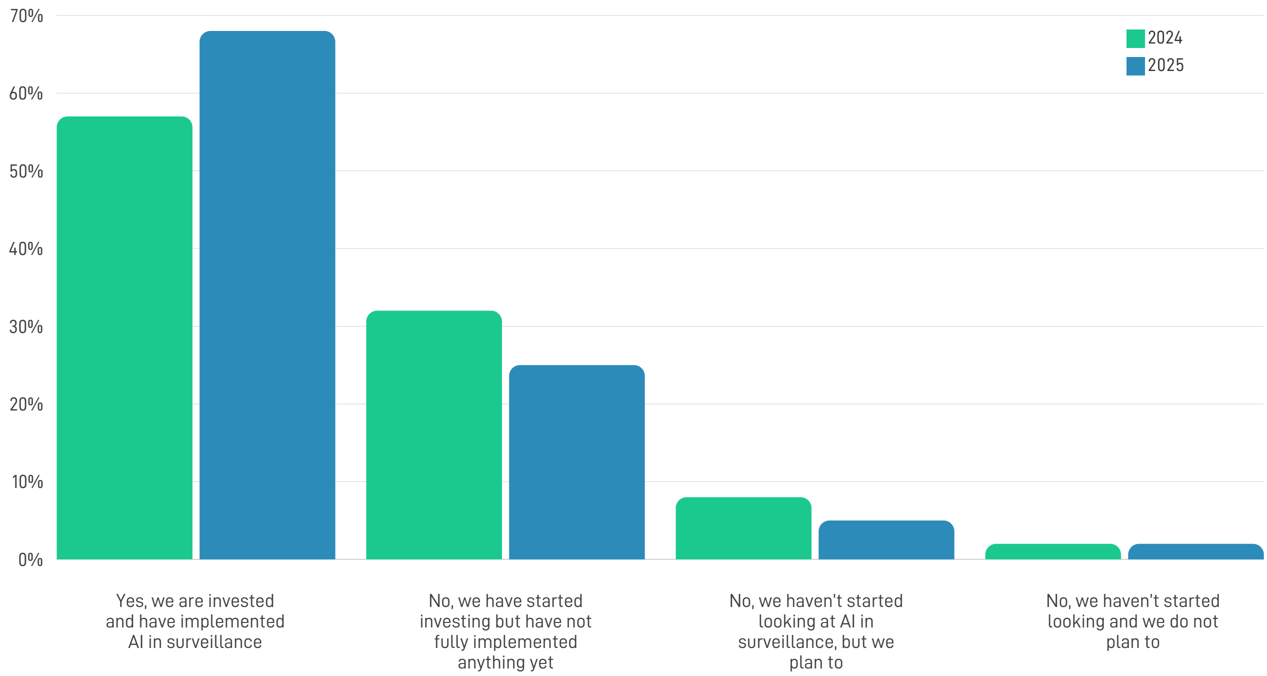


AI Implementation & Impact

Artificial Intelligence (AI) is steadily reshaping the compliance landscape. Coming into 2025, 68% of firms reported that they have already implemented some AI into their compliance processes, while another 25% have begun investing in AI but have not yet fully deployed it.

This marks an increase in adoption compared to the previous year. Only 2% are not looking at AI and have no plans to, indicating an almost universal industry commitment to exploring AI technology.

Have you implemented any Artificial Intelligence (AI) capabilities to improve surveillance processes?



"[AI] allows for leverage and efficiency gains... but we don't always have the budget and we sit behind other teams in terms of priority for access to these tools"

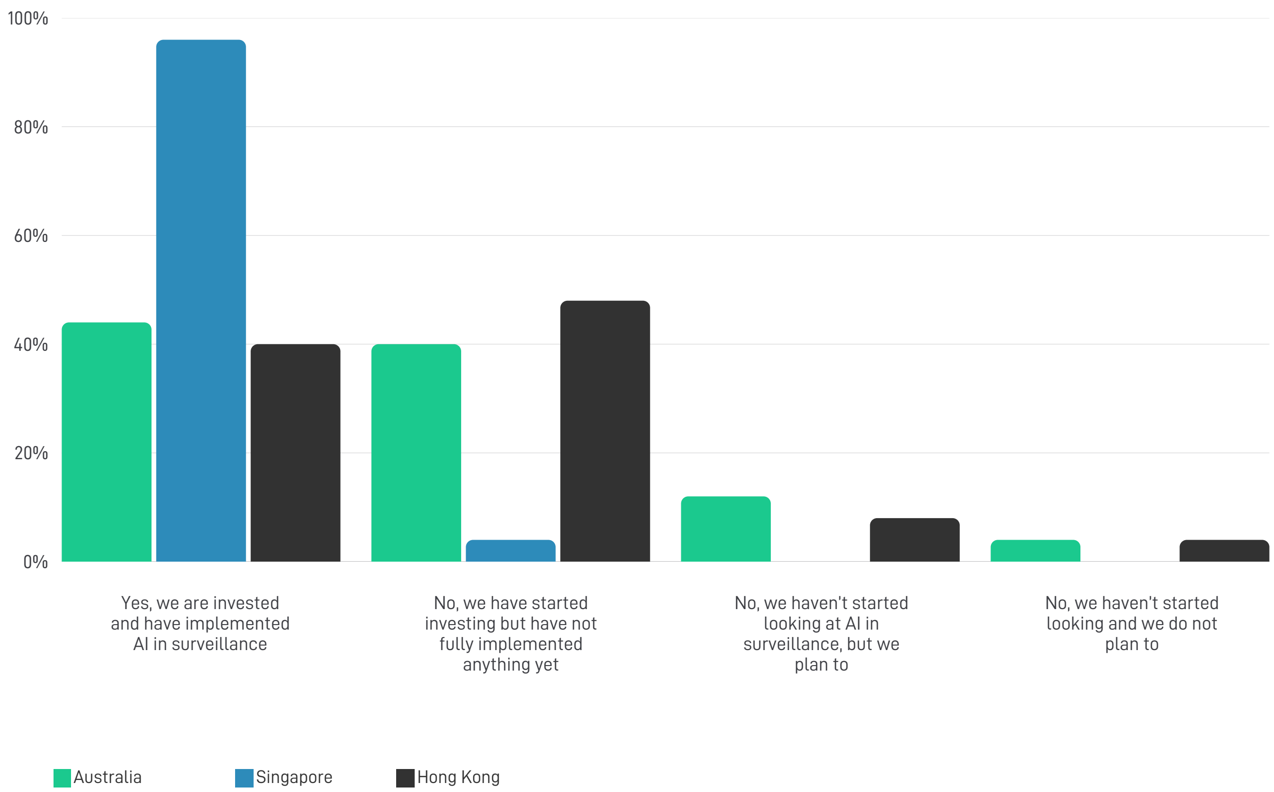
– Chief Compliance Officer at a Global Asset Management Firm

Varying AI adoption across APAC

Aside from Singapore, which actually has the highest level of AI adoption globally at 96%, the rest of the APAC region appears to have been the slowest to adopt AI overall, with Australia and Hong Kong at just 44% and 40% respectively of firms having fully implemented any AI into their compliance processes. This slower adoption suggests some regional differences in either regulatory encouragement, resource availability, or risk appetite for new technology.

Have you implemented any Artificial Intelligence (AI) capabilities to improve surveillance processes?

By firm location - APAC



How Firms are Benefitting from AI

Firms that have implemented AI are already seeing significant improvements in efficiency and effectiveness.

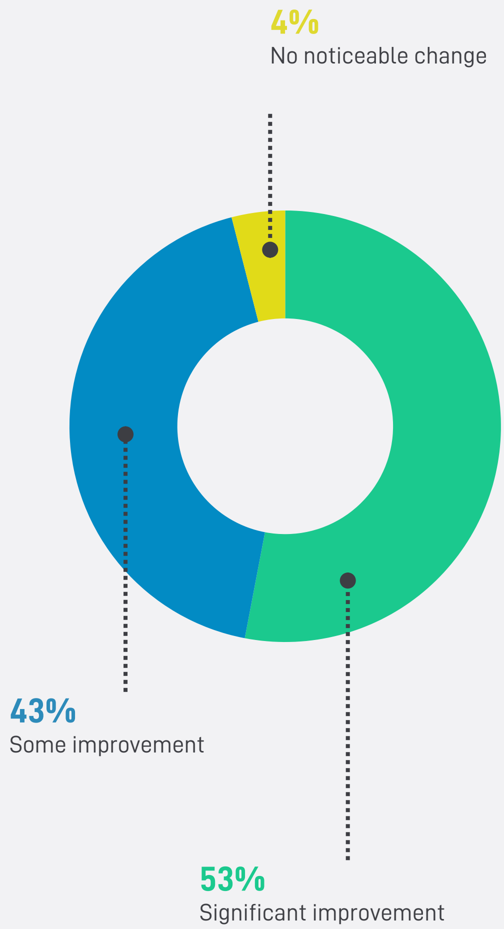
96% report improvements in their compliance processes, and 53% say these improvements are significant. Importantly, not a single company reported any deterioration of their compliance processes due to AI, with just 4% reporting no noticeable change. In other words, for the vast majority, AI has either met or exceeded expectations in terms of boosting compliance effectiveness.

AI is primarily being applied in surveillance alert review, compliance reporting, and data correlation, helping firms streamline manual workloads and identify risk signals more efficiently. As AI models mature, firms are increasingly focused on transparency, auditability, and alignment with regulatory expectations.

AI has quickly moved from concept to reality in compliance functions. Looking ahead, the integration of AI into core compliance processes is expected to accelerate. However, adoption success will depend not only on technology capability but also on data quality, governance structures, and staff training.

Firms that can effectively align AI with business context and regulatory expectations will gain a meaningful advantage, not just in compliance efficiency, but in early risk detection and proactive oversight.

To what extent has your business seen improvement or deterioration in your compliance processes following AI implementation?



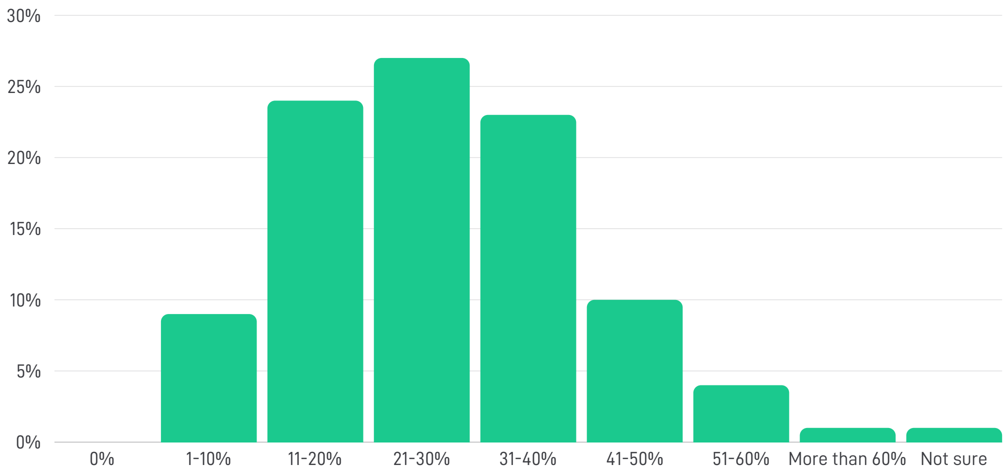
SURVEILLANCE INVESTMENT & RESOURCING

Manual Workloads Across Compliance Teams

Despite continued investment in compliance technology, and the increasing use of AI tools, many firms are still burdened by high levels of manual work.

65% of firms reported a significant portion of their compliance staff (over 20%) are working on administrative or repetitive tasks. This was particularly true in mid-sized and larger firms. A high level of manual work has a direct impact on team capacity, morale, and the ability to scale compliance operations effectively.

What percentage of your firm's compliance staff undertake administrative / manual / repetitive tasks at your firm, if any?



"We always try to automate more where we can. More investments and attention to systems and technology is key [to reducing manual workload]"

– Chief Compliance Officer at a Global Asset Management Firm

The US and APAC had the highest levels of manual workload. 35% of firms in APAC have 31-40% of their compliance staff working on administrative, manual and repetitive tasks, while in the US a small number of firms (3%) reported that more than 60% of their compliance staff undertake these tasks.

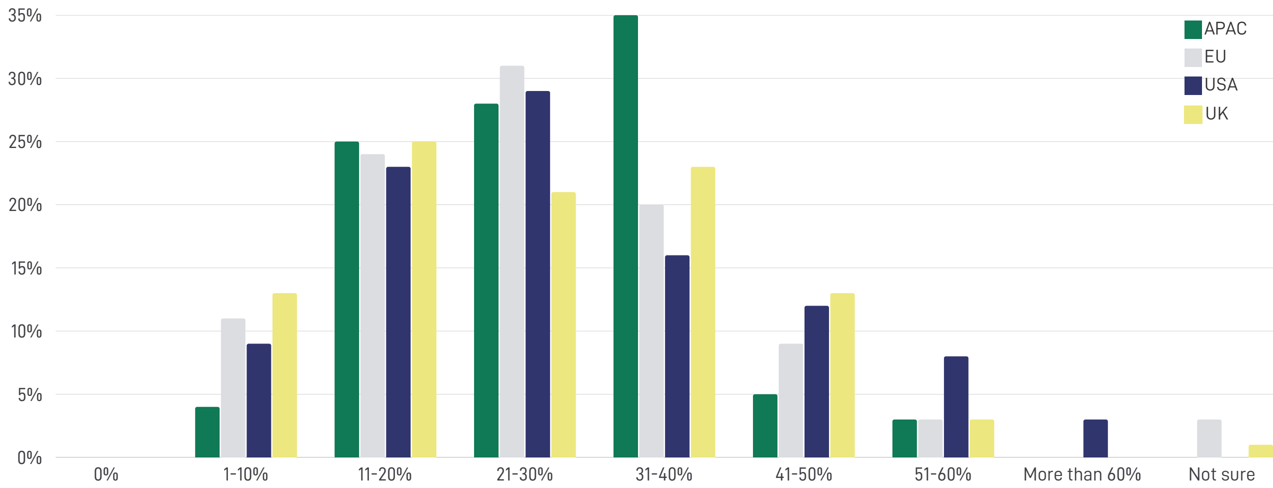
These inefficiencies can contribute to compliance fatigue and increase risk exposure by diverting resources from strategic activities like risk assessment, policy development, and reporting.

Reducing this manual burden remains a key area of focus. The path forward for most firms lies in better integration between systems, adoption of workflow automation, and use of AI or analytics to flag priority issues before they escalate.

While budget growth is encouraging, there are clear opportunities to gain efficiency through automation, workflow streamlining, and better system integration. How firms use that investment, particularly in removing friction from daily compliance workflows, will determine whether teams are able to meet their growing responsibilities without burning out.

What percentage of your firm's compliance staff undertake administrative / manual / repetitive tasks at your firm, if any?

By firm location



Evolving Supervision & Surveillance Models
Overview

As regulatory expectations evolve, firms are adapting their surveillance strategies to account for new communications channels, geographical expansion, and hybrid work environments.

Overall, the picture that emerges is one of transition, as firms upgrade their systems and processes to meet modern communication and conduct risks across distributed teams and markets.

This chapter explores how compliance teams are responding to an ever-growing number of comms channels and a gradual shift in team supervision models

KEY FINDINGS

42% of firms now monitor WhatsApp, surging up the rankings for 2024 to take third spot behind Microsoft Teams and Email

16% of firms are currently surveilling mobile voice calls

58% of firms transcribe voice calls and monitor them via their surveillance system

20% of firms have surveillance systems that only accommodate a single language

35% of respondents rely on sampling and manual review of voice calls

68% of all regulated staff globally are now required to work full-time in the office

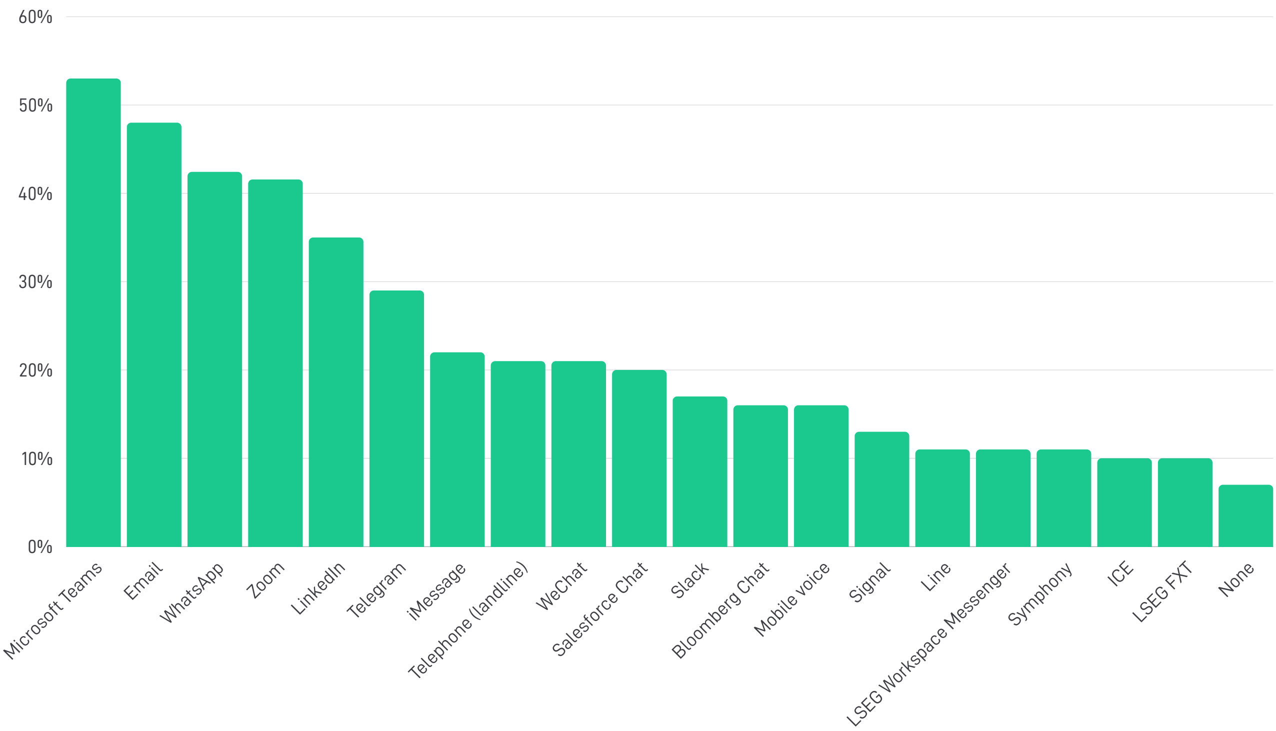
Managing a Proliferation of Comms Channels

The proliferation of diverse communications channels, particularly those operating outside traditional, formally monitored systems, has emerged as a significant and growing compliance risk for financial institutions.

Microsoft Teams (53%) and email (48%) continue to be the two most monitored channels, while WhatsApp (42%) has moved above Zoom to join them on the podium. This was in part driven by a significant rise in UK firms monitoring WhatsApp, jumping by 15% in a single year to 53%.

The growing focus on WhatsApp reflects efforts to capture conversations on encrypted or informal messaging apps that have been a focus of recent regulatory enforcement. Rulings from regulators such as the FCA have moved away from introducing rules to ban the use of WhatsApp and other encrypted apps for unauthorised business communications, leaving firms facing a clear risk if surveillance coverage does not extend to these channels.

What communications channels do you currently capture and monitor, if any?



"The fines involved and client demand to still have conversations on WhatsApp means more of an expectation that this channel be monitored in some way"

– Chief Compliance Officer at a Global Asset Management Firm

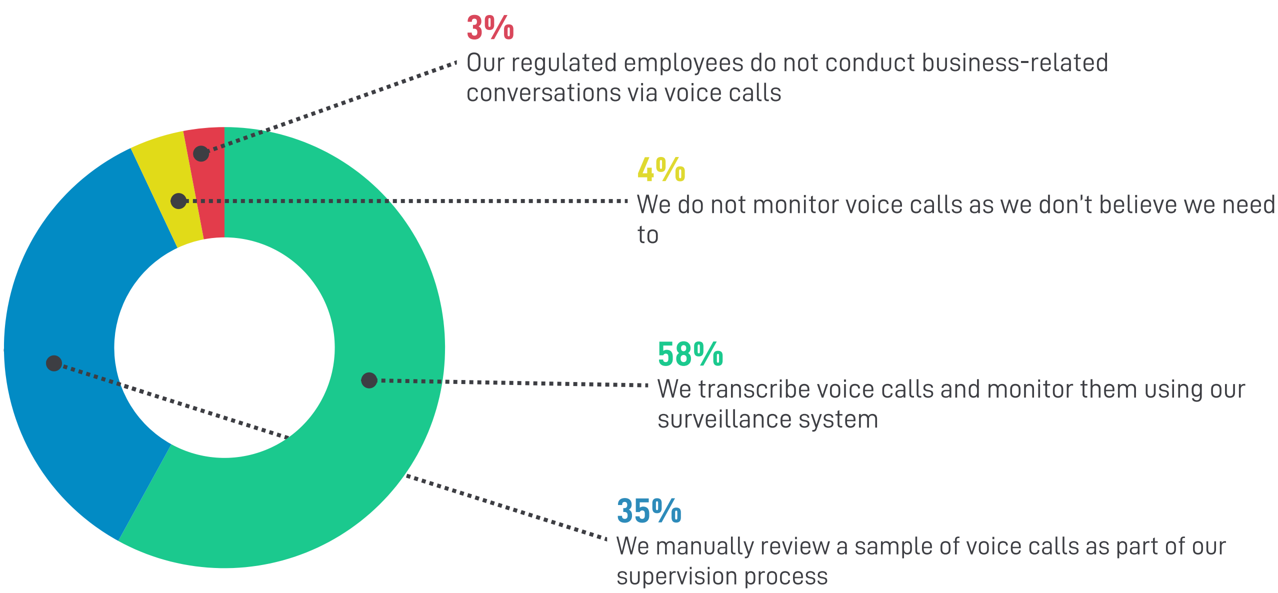
Approaches to Voice Surveillance

Voice monitoring remains a key area of focus. Firms report a variety of approaches to voice surveillance: some rely on manual sampling, others have adopted transcription, while a notable proportion indicate that regulated activity is not conducted via voice at all.

Across all regions 58% of respondents say they transcribe voice calls and monitor them via their surveillance system for market manipulation and conduct risk. 35% manually review samples and 7% are not monitoring voice calls at all. The EU region has the highest instance of manual review with 45% of firms relying on this method to supervise voice calls.

However, looking at the comms channels captured, mobile voice coverage remains at a very low level, with just 16% of firms capturing and monitoring mobile phone conversations. Given how much business is conducted via mobile devices today, this gap could represent a meaningful risk if not addressed.

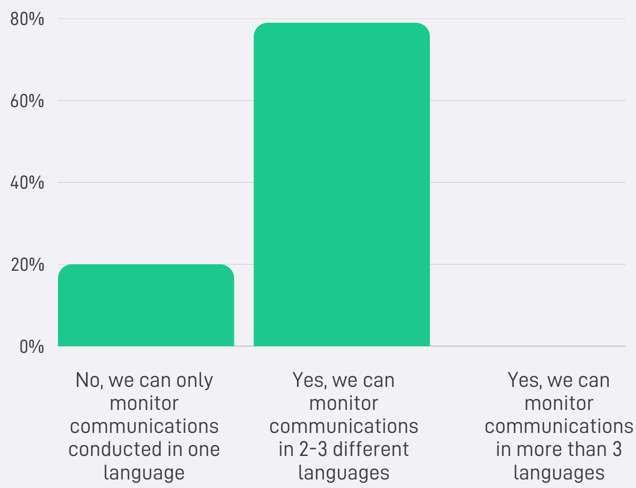
How, if at all, does your firm currently monitor and supervise voice calls for market manipulation and conduct risk?



Language capabilities

Language capabilities are another key area that raises concern. While many firms are expanding their monitoring across two or three languages, 20% still operate surveillance systems that only accommodate a single language, highlighting a clear challenge for global organisations.

Does your firm have the capability to monitor communications in multiple languages for surveillance purposes?



Worryingly, not a single respondent indicated that they could monitor communications in more than 3 languages. Given the number of languages spoken across most global organisations, this is a surprise and a clear concern.

Asset Managers appeared to have the highest risk in this area, with 71% of respondents only able to monitor communications in one language. Such limitations mean that potentially important communications could evade effective monitoring.

"Monitoring voice calls manually does not represent efficient use of resource unless a true risk based approach to sample selection can be identified, or judgement calls need to be made around when to cease listening"

– Head of Compliance Monitoring and Surveillance - Insight Investment

Return to Office

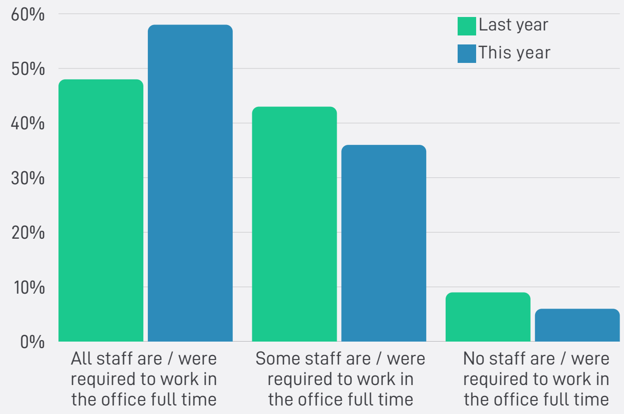
Supervision models are also shifting. The survey results indicate a 10% increase in the number of regulated staff required to work in the office full-time.

The US has seen the biggest increase in back to the office requirements, with 68% of all regulated staff now required to be full-time in the office.

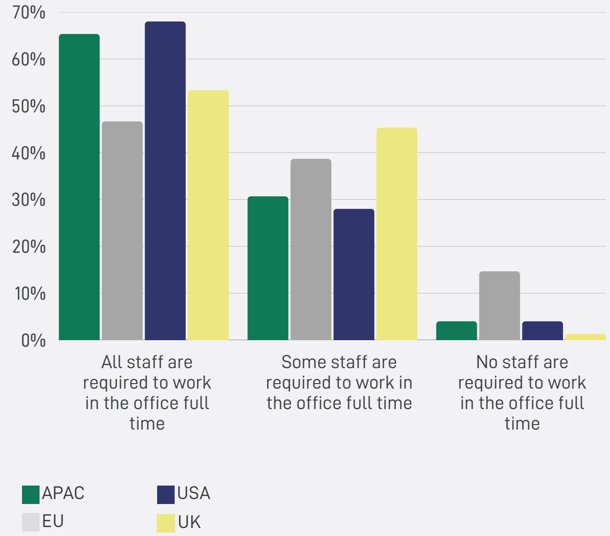
91% of firms noted that their return-to-office requirements for regulated staff were introduced at least in part to improve supervision. In a landscape where communications surveillance remains inconsistent, physical oversight is still viewed as an important control.

Overall, it is clear that supervision and surveillance models are evolving. Compliance teams are actively upgrading their systems and processes to tackle modern communication and conduct risks that come with dispersed teams and digital channels. Traditional supervision methods such as in-person oversight, are being re-emphasised alongside new tech-driven surveillance tools. Firms are blending technology with policy to strengthen their overall supervision frameworks.

Which of the following statements best describes your organisation's requirements of regulated staff compared to a year ago?



By firm location



Communications Surveillance - Responding to Regulatory Action

Overview

Regulatory scrutiny around electronic communications has intensified in recent years, and firms are responding accordingly.

This chapter looks at how compliance teams are thinking about and responding to regulatory action

KEY FINDINGS

67% of respondents expect the volume of fines for communications record keeping failures to increase

71% anticipate the value of fines will increase

32% of firms have fully implemented monitoring of encrypted messaging platforms

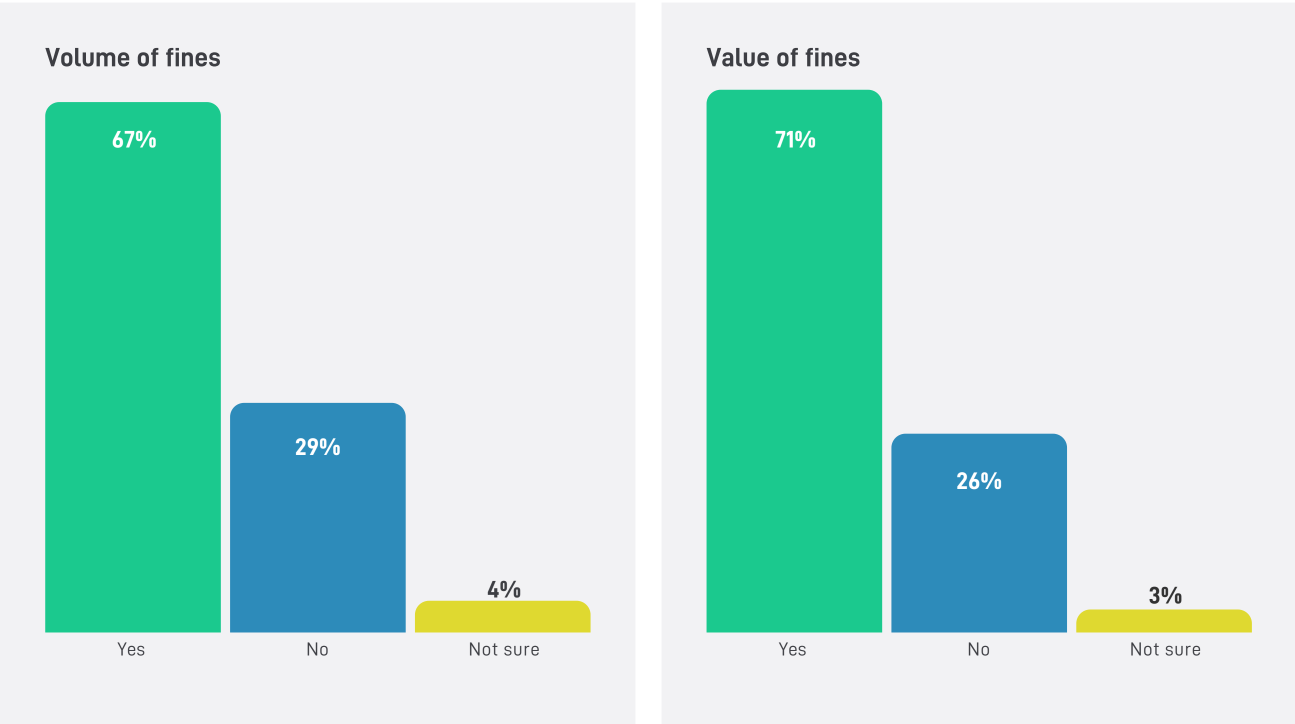
9% of firms are comfortable with their current policies and have made no changes to their electronic communications monitoring in response to increased regulatory scrutiny

Regulatory Enforcement Expectations

In 2025, 67% of respondents expect the volume of fines for communications record keeping failures to increase, and 71% anticipate that the value of those fines will rise.

This is consistent with global enforcement trends, particularly in the US and UK, where despite a shifting regulatory focus, off-channel communications remain a top compliance risk, resulting in a large number of historical fines.

Do you expect regulators to increase the volume and value of fines for e-comms record keeping breaches in 2025?



"[There is] more regulatory attention from regulators in APAC on issues that the SEC and the FCA see. I would expect firms to adjust their practices to be more global and to roll out best practice."

– Chief Compliance Officer at a Global Asset Management Firm

Responding to Off-Channel Communications Risk

When asked how they have responded to off-channel comms enforcement developments, firms cited a variety of approaches:

32% have fully implemented monitoring of encrypted messaging platforms

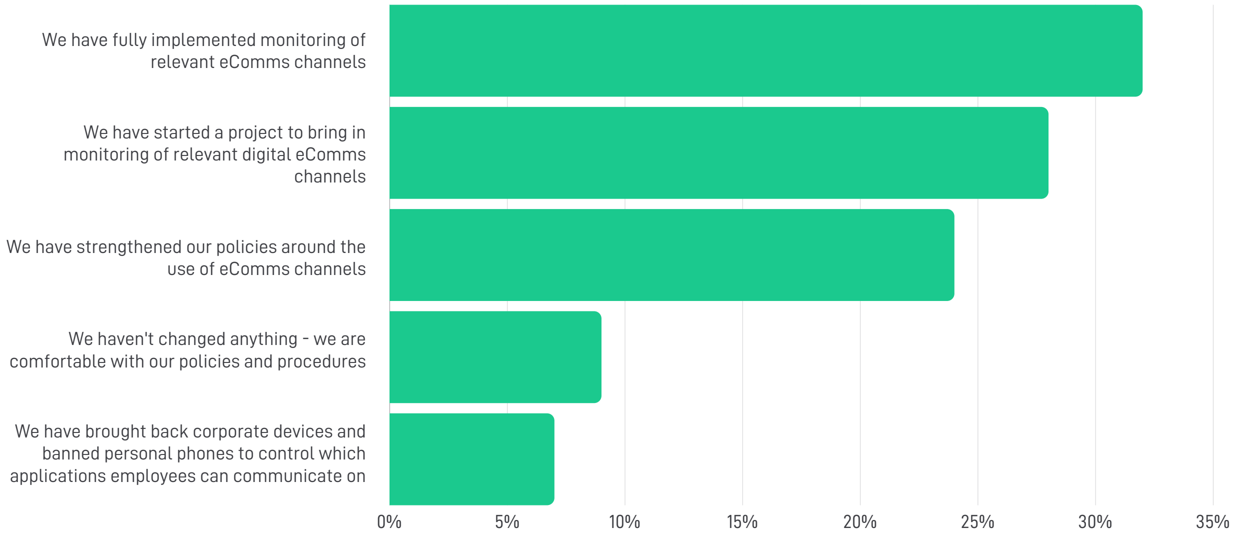
28% have launched projects to bring in monitoring of relevant digital eComms channels

24% have tightened internal policies to restrict or govern usage

7% have reintroduced corporate devices and prohibited personal phones

However, 9% have made no changes and feel comfortable with their current policies.

How, if in any way, has your firm responded to the off-channel communications fines from the last few years around encrypted messaging channels like WhatsApp?



Overall, these figures show that nearly two-thirds of firms are actively investing in better communications surveillance. However, the remaining third may be vulnerable to future regulatory scrutiny, especially if they rely on policy alone without technical enforcement.

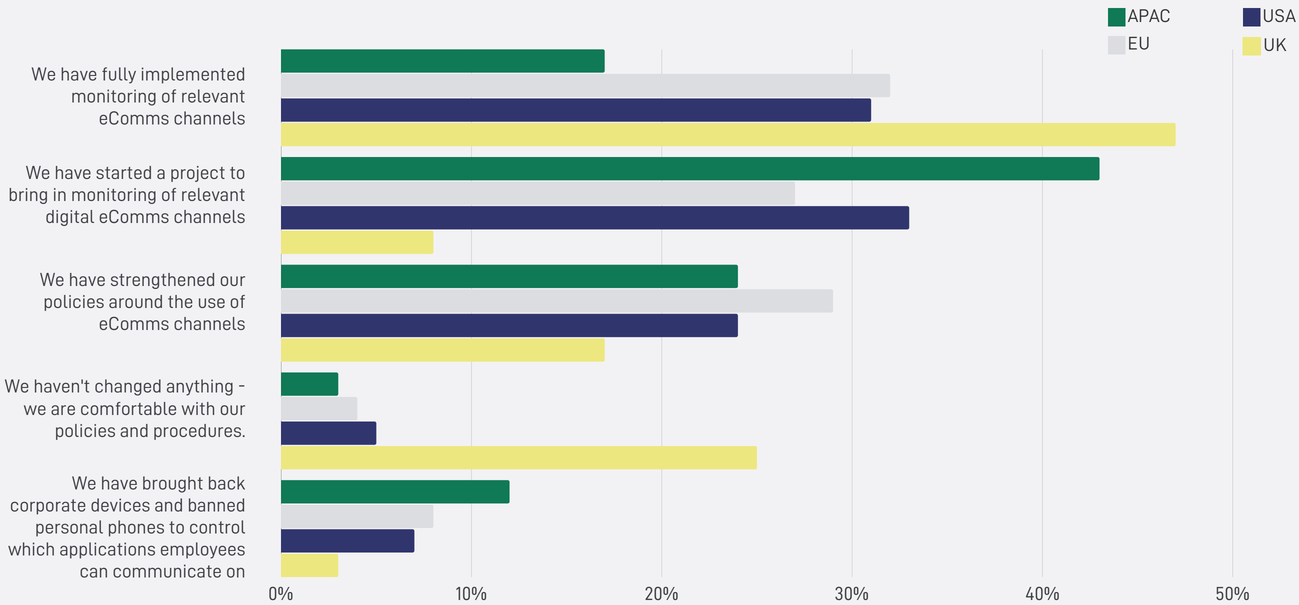
As enforcement activity continues, firms must ensure their compliance controls go beyond documentation. Regulators increasingly expect firms to demonstrate not just that they have policies in place, but that those policies are actively monitored, enforced, and adapted to reflect changing risk.

A Global View

Firms around the world are taking action to respond to regulatory crackdowns on encrypted communications channels, but the form and speed of these responses vary widely.

How, if in any way, has your firm responded to the off-channel communications fines from the last few years around encrypted messaging channels like WhatsApp?

By location



"[In response to these changes], firms should persist with a robust risk management approach. Reactionary actions are not looked well upon by the regulator."

– Chief Compliance Officer of a Multinational Investment Bank and Financial Services Firm

In the UK, nearly half of all firms (47%) have already fully implemented monitoring of encrypted messaging channels like WhatsApp. However, 25% reported taking no action, citing confidence in their existing policies.

In the US, a more mixed approach is evident: 33% of firms are currently implementing projects to introduce monitoring, 31% have fully implemented solutions, and 24% have strengthened internal policies.

Across continental Europe, French and German firms are broadly proactive. In Germany, 40% of firms launched monitoring projects, while 24% had fully implemented tools. France shows similar activity, with 36% having fully implemented and 24% revising policies.

Singapore stands out for forward-looking action: 72% of firms said they have initiated a project to implement monitoring, the highest among all regions, though just 12% had completed implementation at the time of the survey.

Hong Kong showed the highest rate of device control responses, with 24% of firms reissuing corporate devices to limit use of personal messaging apps.

The APAC region as a whole had the lowest levels of confidence in their current policies and procedures, and only 17% had fully implemented monitoring of relevant eComms channels. With over 70% of APAC firms expecting both the volume and value of fines to increase in 2025, there is still a lot to do.

This regional variation underscores the different compliance postures, regulatory expectations, and operational readiness across jurisdictions, and highlights where regulators may push harder for enforcement follow-through.

Looking Ahead: Priorities & Preparedness
Overview

Despite the challenges facing compliance teams, there is a strong sense of momentum heading into 2025.

When asked to identify their top compliance priority for the next 12 months, firms focused on:
- Enhancing data quality for Board-level reporting
- Integrating AI into alert review and surveillance
- Managing regulatory change and project implementation

These priorities reflect a shift in focus from simply maintaining compliance to elevating it through better insight, more automation, and smarter resource allocation.

This chapter unpacks how compliance teams are thinking about and responding to regulatory action.

→ Cultural Drivers of Compliance

→ Growing Confidence

→ Surveillance Systems Under Review

KEY FINDINGS

37% of firms are completely confident their system captures all relevant records

80% of firms plan to upgrade or replace their surveillance technology in 2025

37% of firms consider the risk of reputational damage as the strongest deterrent against non-compliance

27% of firms are primarily concerned with the cost of financial penalties and remediation

Cultural Drivers of Compliance

Compliance culture plays a critical role in shaping how firms approach and respond to risk, and what ultimately drives them to maintain regulatory integrity. It plays a pivotal role in guiding employee behaviour and ensuring that adherence to regulations is more than just a box-ticking exercise.

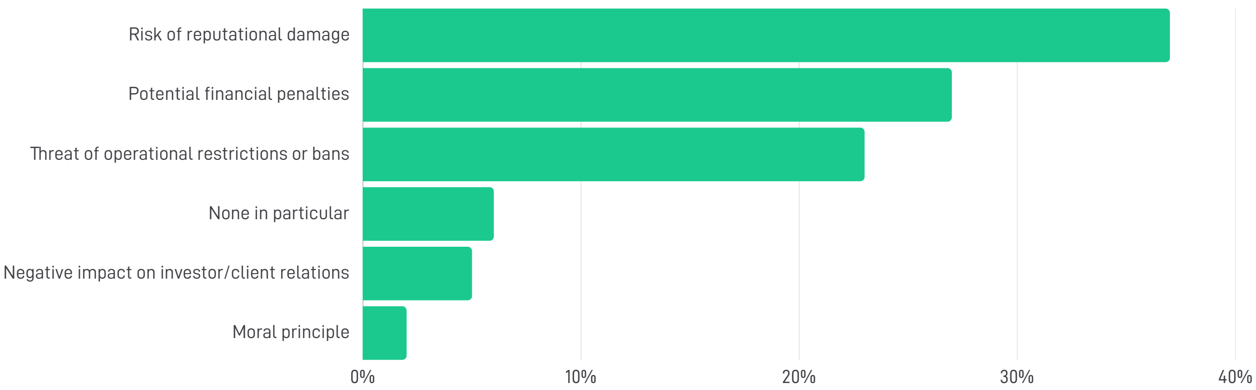
When asked what serves as the strongest deterrent against non-compliance within their organisation, firms most commonly cited:

37% the risk of reputational damage

27% the cost of financial penalties and remediation

23% the threat of operational restrictions or bans

What, if anything, is the strongest deterrent for your financial institution against non-compliance?



These responses suggest that both external pressure from regulation and internal commitment to brand reputation are important in driving compliant behaviour. While fear of fines remains a motivator, many firms recognise that long-term trust with clients, regulators, and the public hinges on doing the right thing, not just avoiding enforcement. Losing trust due to a compliance failure (especially a public one) can be more damaging in the long-run than one-off fines.

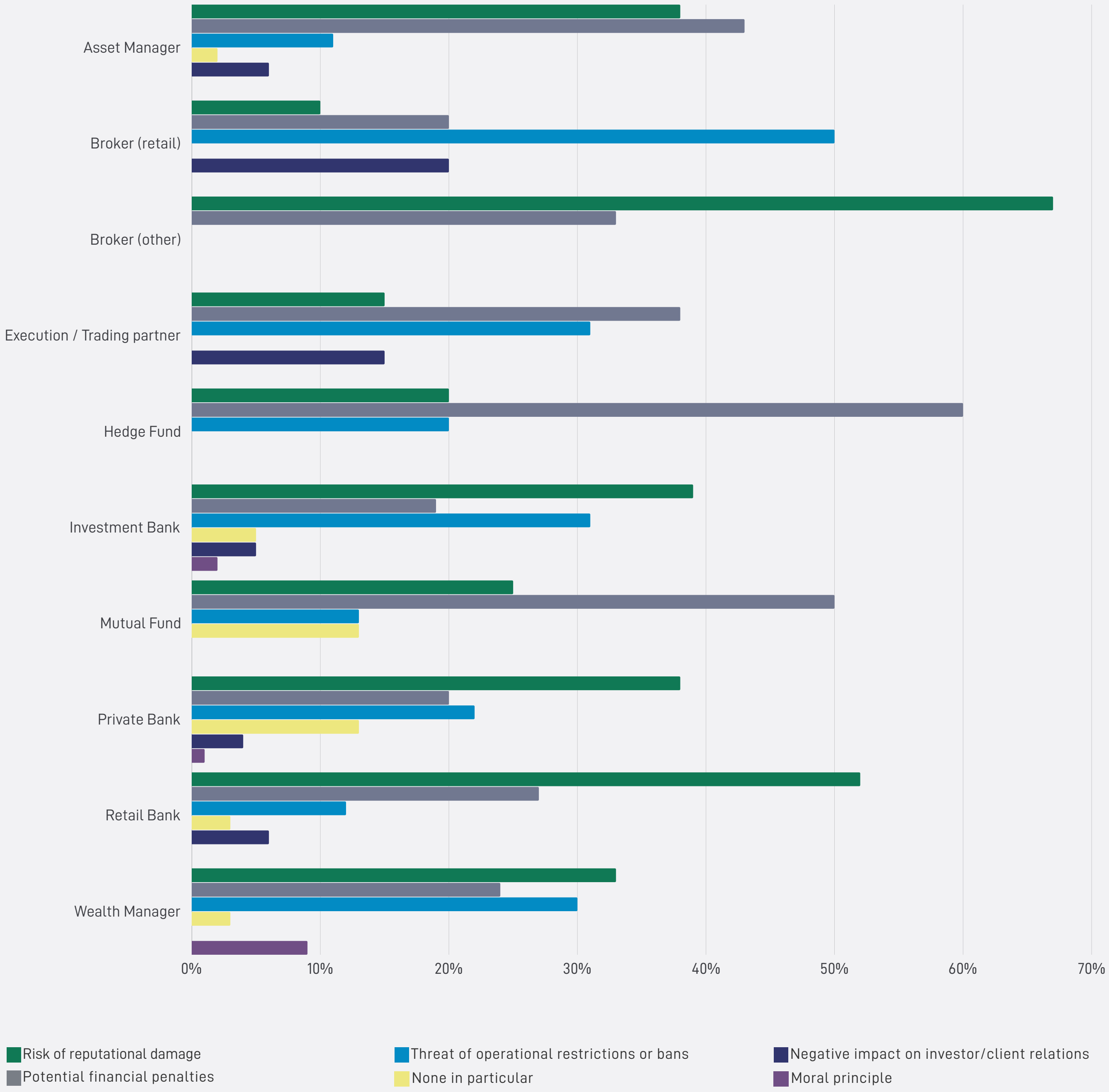
Building a strong compliance culture requires more than policies and surveillance. It requires leadership engagement, clear communication of expectations, and ongoing education to empower employees at every level to uphold standards.

As regulators continue to emphasise the importance of 'tone from the top', firms that foster an open and ethical culture will be better positioned to identify risks early, resolve issues transparently, and sustain regulator and client trust over time.

Differences by Firm Type

Hedge Funds, Mutual Funds and Asset Managers are the most concerned about financial penalties, with 60%, 50% and 43% respectively citing this as the leading deterrent against non-compliance.

Retail Brokers stood out for their sensitivity to enforcement: 50% said the threat of operational restrictions or bans was their top compliance motivator. Meanwhile, 20% focused on avoiding damage to investor or client relationships.



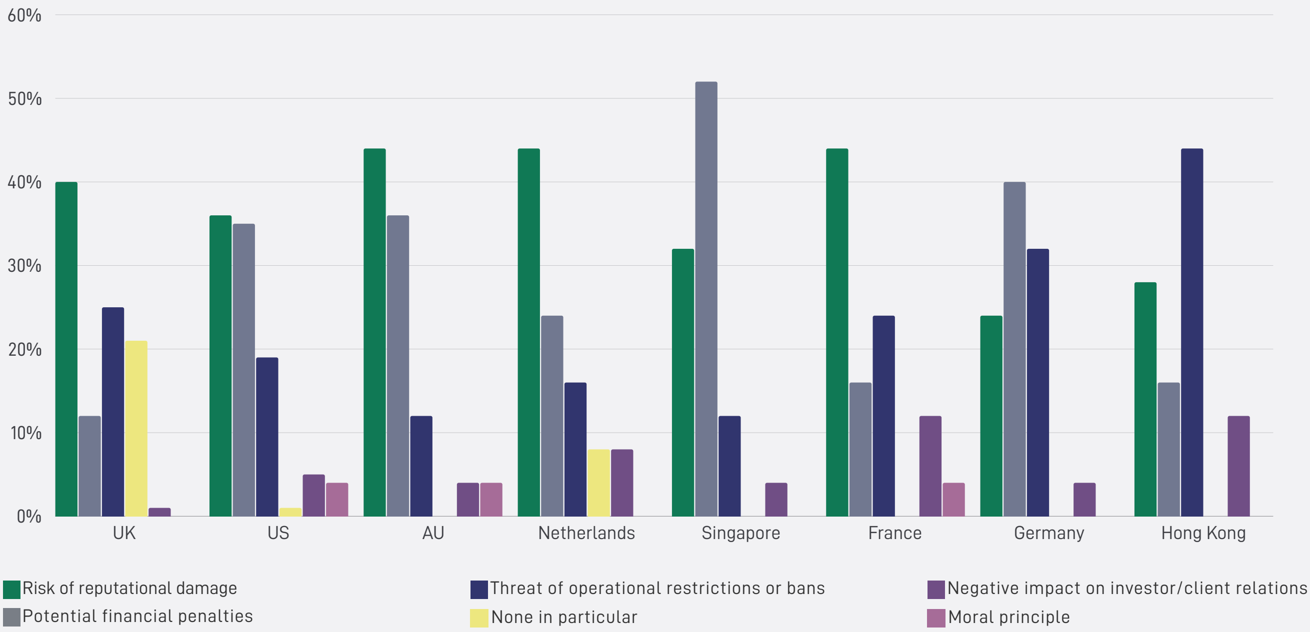
Cultural Drivers of Compliance

Regional Variations

In the UK and USA, reputational damage was the top concern. 40% of UK firms and 36% of US firms selected it as the leading driver. In Europe, France (44%) and the Netherlands (44%) also leaned toward reputational risk. German firms were more mixed: 40% cited financial penalties while only 24% named reputational damage.

Singapore leaned more heavily on regulatory consequences, with 52% of firms citing financial penalties versus 32% for reputational damage. Hong Kong, however, showed the reverse: 28% of firms are most concerned about reputational damage and 16% focused on penalties.

By firm location



Operational restrictions were a notable concern in Hong Kong (44% of firms), Germany (32%), and the UK (25%). These jurisdictions may be more attuned to supervisory enforcement linked to license conditions or trading limits.

Client trust also featured in several countries, particularly France, the Netherlands and Hong Kong while moral principles were a minor driver overall (just 3 responses globally).

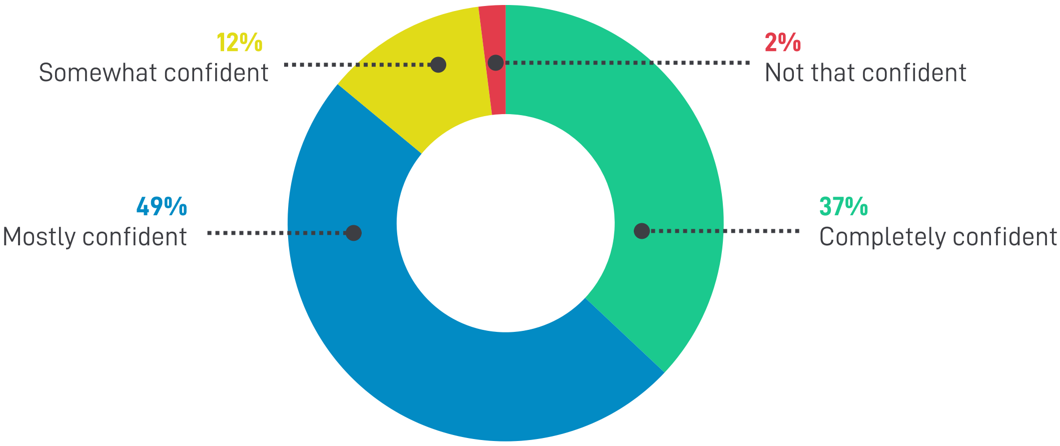
These patterns suggest that while the cultural foundation of compliance is broadly strong, regulatory pressure, business continuity and enforcement exposure continue to shape behaviour in market-specific ways.

Growing Confidence

Confidence in surveillance coverage is relatively high, with 37% of firms feeling completely confident their current surveillance system captures all relevant records.

49% are mostly confident, 12% report being somewhat confident and just 2% admit they have low confidence in their surveillance coverage.

How confident are you that your surveillance system is surveilling all of your business records?



While these results are encouraging, and most firms feel they are on the right path, they also signal an opportunity. The gap between 'mostly confident' and 'completely confident' reflects ongoing challenges around system integration, data governance, and user adoption. The challenge now is turning this optimism into long-term results through continuous and prioritised investment in systems, processes, and people.

The firms that succeed in building flexible, forward-looking surveillance strategies, grounded in automation and analytics, will be better equipped to meet future regulatory expectations and operational complexity.

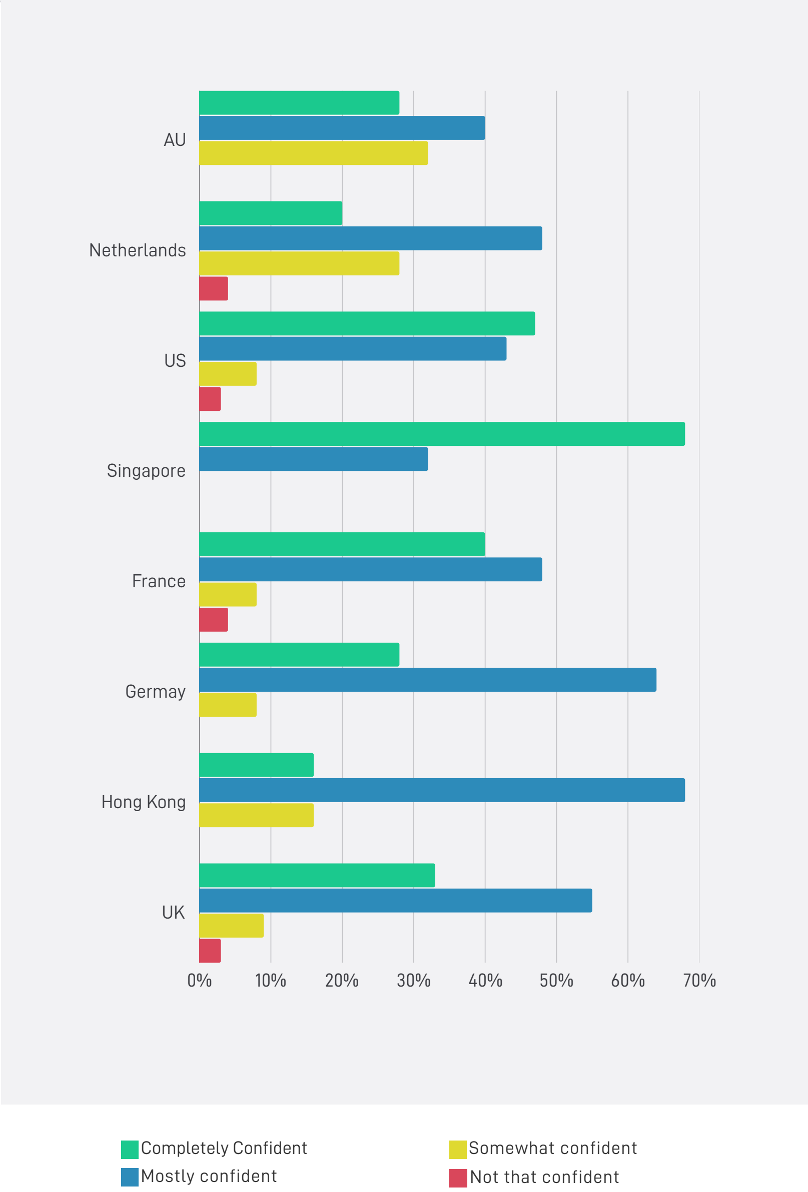
As regulatory expectations continue to evolve, preparedness will depend not only on technology, but on how well firms can align strategy, systems, and culture to anticipate and adapt to change.

Regional Confidence Levels

Across regions, confidence in firms' surveillance system coverage is relatively consistent. Singapore has the highest levels of confidence with an impressive 100% of firms being mostly or completely confident they are surveilling all of their business records. In neighbouring Hong Kong, however, only 16% are completely confident in their coverage, while a strong 68% are mostly confident.

Confidence is lowest in France and Netherlands, with 4% not at all confident of their surveillance coverage. The UK and US are just behind at 3%.

These findings suggest that while strategic investment is increasing, many firms still feel underprepared. Building confidence in surveillance systems will require both technical integration and assurance processes that withstand regulatory scrutiny.



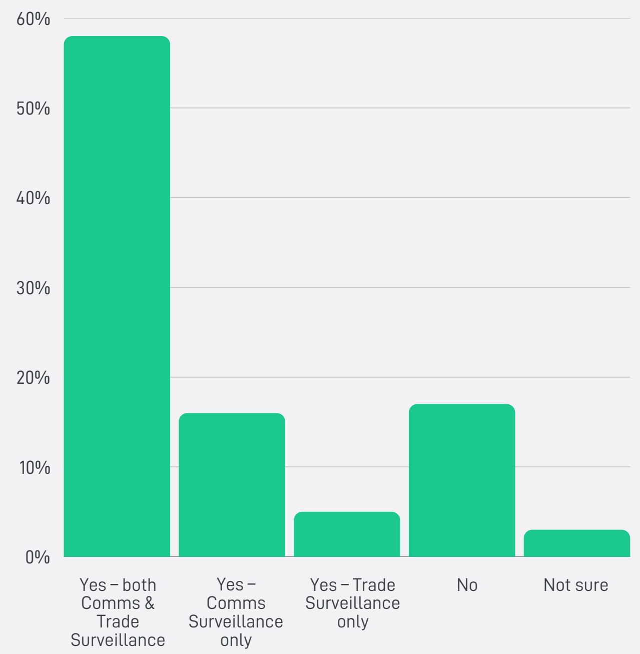
Surveillance Systems Under Review

As compliance risks grow in complexity, firms are re-evaluating the systems they rely on to monitor communications and trading activity.

80% of firms reported plans to upgrade or replace their surveillance technology in 2025. Some are seeking to consolidate their systems to reduce vendor sprawl and improve overall efficiency, while others are focused on adopting more flexible and integrated platforms that can adapt to changing regulatory and operational needs.

This reflects a wider recognition that legacy systems, often siloed and difficult to scale, are no longer sufficient. Modern compliance environments are now expected to support everything from early risk detection to board-level MI and audit preparedness, and require tools that can seamlessly connect communications, trade, and behavioural data at speed.

Are you looking to replace your surveillance solution(s) in the next 12 months?



Conclusion

The 2025 SteelEye Compliance Health Check paints a picture of a compliance function that is both under pressure and actively evolving.

Teams are grappling with increasingly complex regulations, operational constraints, and the continued shift to digital communications and hybrid work. Yet across the board, firms are responding - with investment, with innovation, and with a growing belief that smarter, more connected compliance is possible.

The survey results point to a clear inflection point: budgets are rising, AI is being integrated, and firms are taking proactive steps to improve surveillance and reduce manual workloads.

But high confidence must be matched by action. To stay ahead, firms must focus not just on expanding surveillance, but on making it meaningful by connecting systems, improving data quality, and delivering insights that support risk-informed decision-making at every level.

There are also some noteable gaps. Voice surveillance, especially on mobile, and multi-language monitoring capabilities remain limited, exposing firms to significant blind spots. Indeed, none of the firms surveyed reported surveillance capabilities in more than three languages, highlighting a critical vulnerability in an increasingly global and multilingual market.

While it's clear many firms are investing in best-in-class tools with a steady shift toward integrated surveillance strategies, the results also reveal gaps in integration and overlay, particularly when it comes to joining communications and trading data to enable true holistic oversight.

The firms that succeed in this next phase will be those who view compliance not simply as a control function, but as a source of strategic intelligence that is critical to operational resilience, regulatory trust, and long-term performance.

About SteelEye

SteelEye provides a comprehensive integrated platform, bringing together communications and trade surveillance, record keeping, regulatory reporting, and analytics in one unified solution.

Trusted by over 200 financial firms globally, including tier-one banks, asset managers, hedge funds, and brokers, SteelEye helps compliance teams achieve deeper insight, greater efficiency, and stronger oversight.

With support for voice and electronic communications across channels like WhatsApp, Bloomberg, Microsoft Teams, and more, SteelEye enables firms to capture, monitor, and analyse their data for effective compliance. Its powerful AI automation and analytics tools reduce alert fatigue, accelerate investigations, and provide the intelligence needed to manage risk proactively.

SteelEye is committed to helping firms stay ahead of regulatory change, reduce compliance costs, and build long-term resilience through smarter technology and expert support.

To learn more, visit www.steel-eye.com

Technology Excellence

We offer the only truly integrated surveillance solution in the market. Our platform provides top-of-the-range deployment options, including public or private cloud, ensuring flexibility and scalability. With resilient and robust infrastructure, coupled with the highest security standards, our surveillance, record keeping and reporting solutions provide ultimate peace of mind.

Leading Expertise

At SteelEye, we pride ourselves on having the brightest minds across technology, regulation, and compliance. Our team boasts diverse expertise and skill sets, allowing us to deliver innovative solutions tailored to our clients' needs.

With a global team, we bring together talent from around the world to provide unparalleled expertise and support.

Global Reach

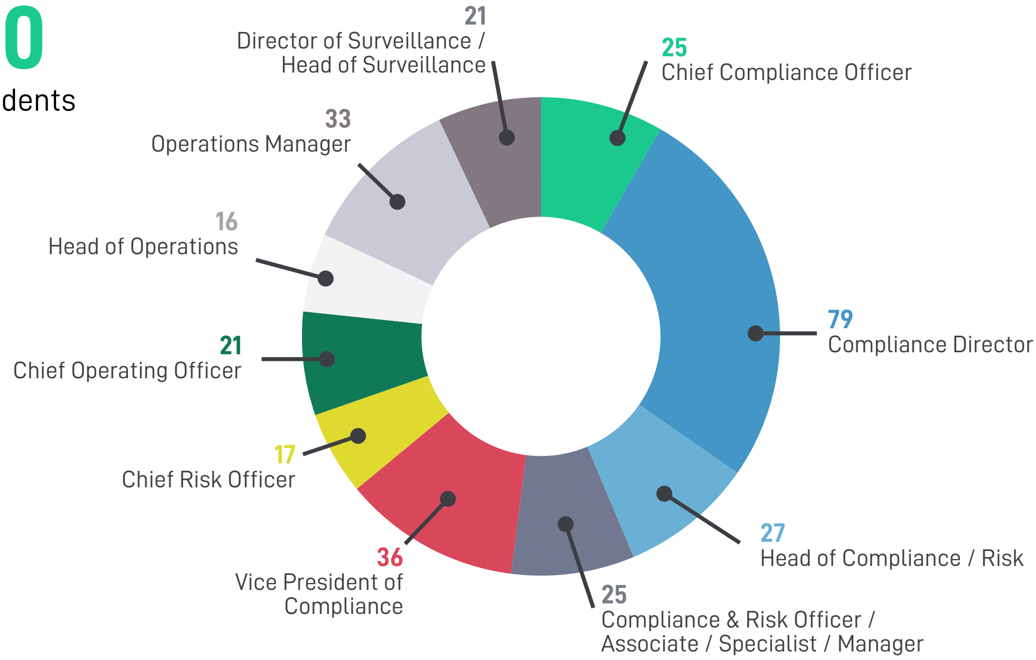
With a global presence across UK, EMEA, US and APAC, we have established ourselves as a trusted compliance partner across the financial industry.

Firms across the globe rely on SteelEye to demonstrate compliance mastery and effortlessly navigate the complexities of the regulatory landscape.

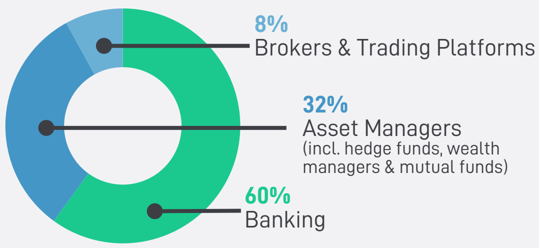
Methodology & Respondents

The research was conducted by Censuswide, with 300 Senior Compliance Decision Makers within Financial Services firms across Australia, Singapore, Hong Kong, France, Germany, Netherlands, UK and USA. The data was collected between 31.01.2025 – 04.02.2025. Censuswide abides by and employs members of the Market Research Society which is based on the ESOMAR principles. Censuswide are also members of the British Polling Council.

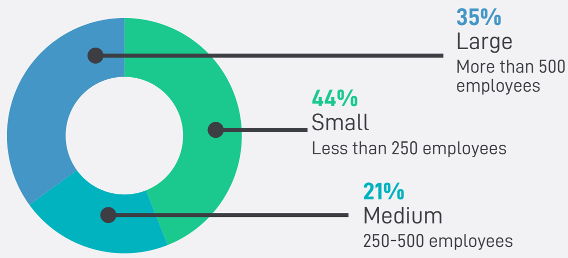
300
respondents



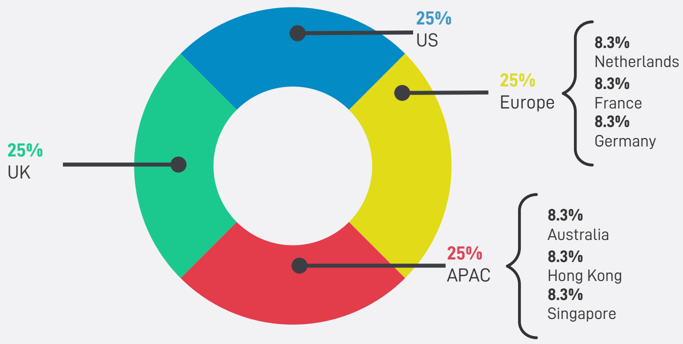
By firm type



By firm size



By firm location



SteelEye

2025 Annual Compliance Health Check Report

www.steel-eye.com