



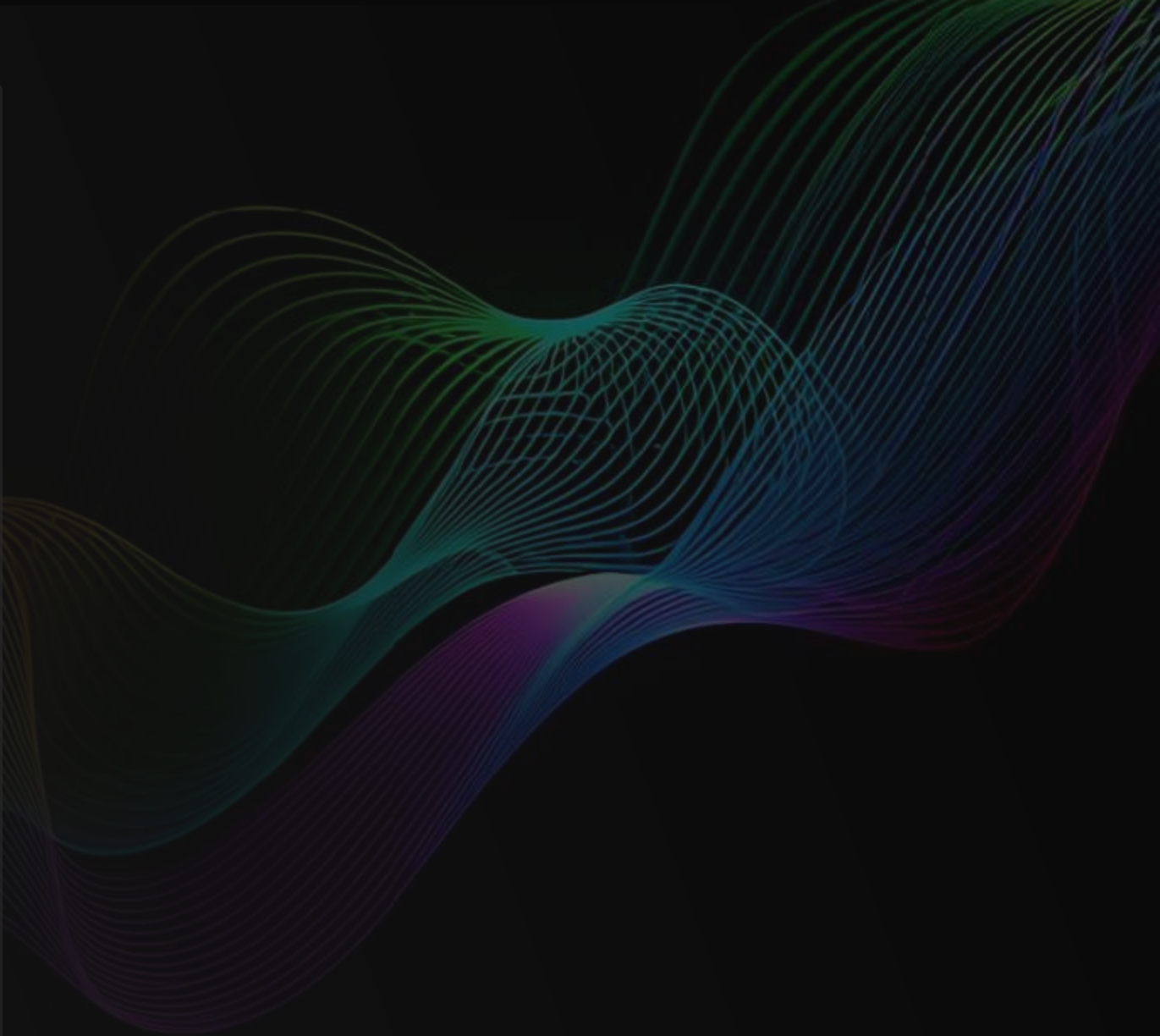
AML
Intelligence

FinCrime Frontier 2026–27

The state of financial crime compliance:
regulation, performance, AI, and the path ahead

Contents

Foreword	3
Executive summary	4
Methodology and respondent profile	7
CHAPTER 1: The new financial crime landscape	9
CHAPTER 2: From regulatory change to regulatory adaptability	14
CHAPTER 3: The economics of compliance	21
CHAPTER 4: Operational performance: Closing the effectiveness gap	27
CHAPTER 5: AI moves from experimentation to enterprise capability	33
CHAPTER 6: The future financial crime operating model	40
Conclusion: From AI ambition to operating reality	44
Acknowledgment of contributors	45



Foreword

Financial institutions are making substantial investments in AI. Yet many struggle to show how that investment is turning into measurable improvements in financial crime compliance.

Over the past several years, the conversation has moved rapidly from the potential of AI to its practical application across transaction monitoring, sanctions, KYC and investigations. Today, the question for financial crime leaders is increasingly not whether AI will play a role, but how it can be deployed responsibly and at scale to improve outcomes.

The FinCrime Frontier 2026–27 research results reflect that shift.

Based on the perspectives of more than 200 financial crime and compliance leaders, including senior leaders from major global financial institutions, the findings reveal an industry with significant ambition, but also one confronting the realities of execution. Institutions are investing in AI and automation while continuing to address the data, technology, governance and operating-model constraints that determine whether innovation can translate into sustainable value.

That translation is not guaranteed. Applying new technology to existing processes and systems can make those processes faster – without making the financial crime function more effective.

The greater opportunity is not speed. It is rethinking how financial crime risk is identified, how intelligence is connected, how controls respond to changing threats and how investigators make more informed decisions. It is also an opportunity to reconsider where

human expertise creates the greatest value as AI takes on more operational activity.

That shift raises important questions for leaders. How should institutions measure the effectiveness of increasingly AI-enabled controls? How can they capture efficiency gains without compromising regulatory assurance? How should AI decisions be governed, explained and challenged? And how can operating models become more adaptive as financial crime threats and regulatory expectations continue to evolve?

These questions sit at the heart of this year's research.

Across the findings, effectiveness, efficiency and explainability emerge as interconnected requirements for the next phase of financial crime transformation. Improving one in isolation will not be enough. Efficiency without effectiveness risks accelerating activity without improving outcomes. Effectiveness without explainability becomes increasingly difficult to govern and defend. None can be sustained without the data, technology, skills and governance required to support them.

Resilience and adaptability are equally important. Financial crime does not stand still. Typologies evolve, payment ecosystems change, transaction volumes grow, and regulatory expectations continue to develop. Yet many compliance programs still assess risk and update controls through periodic review cycles. Closing that gap will require financial crime controls and operating models that can respond to changing risk with greater speed and precision.

The research also points toward a broader evolution of the financial crime function. The future will not be defined by automation alone, nor by autonomy for its own sake. It will depend on how effectively institutions connect intelligence, detection, investigation and governance so that controls can respond as risk changes, while

maintaining appropriate human oversight and accountability.

AI can be a powerful enabler of that transition. But AI itself is not the transformation.

For financial crime leaders, the next phase is therefore about moving from experimentation to execution and from technology adoption to demonstrable impact. The greatest value will come from translating innovation into measurable compliance outcomes, supported by the governance, transparency and resilience needed to scale with confidence.

For MLROs, Heads of Financial Crime and the wider teams shaping financial crime strategy and transformation, we hope this research provides a useful benchmark for evaluating priorities, investment decisions and operating-model choices and for understanding where the industry stands today and where it is heading.

We would like to thank the financial crime and compliance professionals who contributed their perspectives to this research, as well as the teams at SymphonyAI and AML Intelligence who brought the study and report together. Their experience and insight have helped ground this research in the challenges and opportunities financial crime leaders are navigating today.



John Edison
President of Financial
Services, SymphonyAI



Stephen Rae
Co-Founder and Chair,
AML Intelligence

Executive summary

From AI ambition to measurable impact

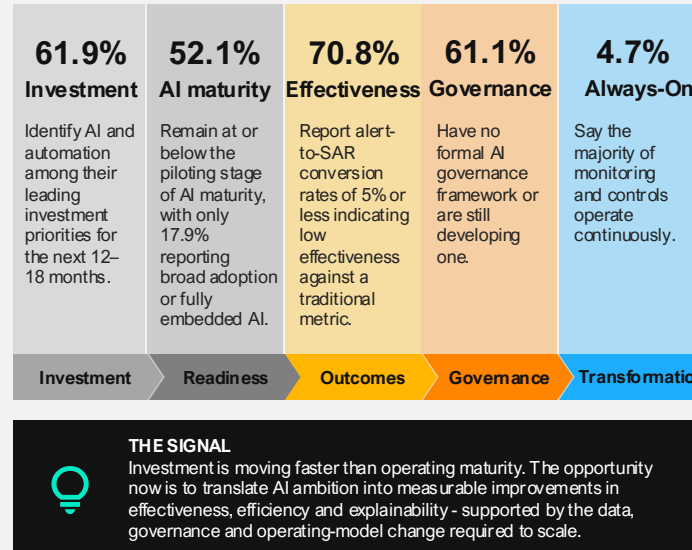
FinCrime Frontier 2026–27 reveals a clear gap between the industry's ambition for AI and its readiness to deliver that ambition at scale.

Based on the perspectives of more than 200 financial crime and compliance leaders across EMEA and the Americas, the research finds that AI and automation are now the leading investment priority, cited by 61.9% of respondents. Yet 82.1% of organizations remain at or below the piloting stage of AI maturity, while the same proportion report that no more than half of their financial crime processes are automated.

Across the findings, the challenge is shifting from adoption to impact: improving effectiveness, delivering efficiency and maintaining explainability while building more resilient and adaptive financial crime operations.

FINCRIME FRONTIER 2026–27 | AT A GLANCE

AI ambition is accelerating. Operational maturity still has ground to cover.



Five findings stand out.

1. AI investment has moved ahead of operational maturity

AI has moved firmly into the financial crime investment agenda, but enterprise maturity has yet to catch up. AI and automation now rank ahead of data integration, RegTech, talent and workflow modernization as an investment priority.

Adoption is also expanding across practical financial crime use cases. Transaction monitoring leads current AI adoption at 56.1%, followed by sanctions at 45.5%, while use across fraud and KYC/CDD is also growing.

Yet broad enterprise adoption remains limited, and automation levels show a similar pattern. The next challenge is execution: moving successful use cases beyond experimentation, integrating them into end-to-end workflows and establishing the data, governance and operating foundations required to scale.

2. The effectiveness gap remains unresolved

Institutions face a growing pressure to demonstrate effectiveness through measurable outcomes and evidence. The survey suggests that some operational performance is improving, structural constraints in data, technology, and automation limit progress.

Alert management provides a clear example. 70.8% of respondents report alert-to-SAR conversion rates of 5% or less, underscoring the volume of investigative activity that does not ultimately result in regulatory reporting and reinforcing the need to examine detection quality alongside processing efficiency.

False-positive performance reveals another measurement challenge. More than one in five

respondents do not track false-positive rates at all, while reported rates vary widely among those that do. At the same time, detection accuracy ranks among the most widely used effectiveness KPIs,

3. Regulatory pressure is reshaping the modernization agenda

Financial crime leaders are being asked to modernize while responding to an increasingly complex regulatory environment.

AI and model governance and the adequacy of technology and systems are the most frequently cited regulatory challenges, each selected by 40.8% of respondents. Cross-border regulatory complexity, the pace of regulatory change and the growth of real-time payments add further pressure.

Yet institutions vary considerably in how they are responding. 26.5% say regulatory change is primarily increasing reactive workload, compared with 20.4% who say it is accelerating transformation. Engagement with regulators around technology and AI also remains limited: only 18.4% describe their engagement as collaborative or leading.

Regulatory assurance and modernization should not be treated as competing objectives. Increasingly, modernization needs to support both stronger

compliance outcomes and greater regulatory confidence.

As AI becomes embedded more deeply in financial crime operations, MLROs will need to demonstrate not only that new capabilities improve performance, but that their use is governed, validated, explainable and aligned with regulatory expectations.

4. Data, governance and explainability will determine whether AI can scale

The barriers to scaling AI increasingly lie in the foundations required to support it.

Data quality and integration ranks as the leading operational barrier, cited by 52% of respondents, and the leading barrier to AI adoption at 50.4%. Yet only 12.4% of organizations describe their data readiness for AI as strong, advanced or leading.

Governance maturity also trails adoption. 61.1% of respondents either have no formal AI governance framework or are still developing one, while only 14.1% report a fully operational framework.

Explainability presents a related challenge. Institutions currently rely most heavily on documentation and audit trails and manual review, while dedicated explainable-AI tools remain less widely adopted.

These are no longer supporting technology considerations. Data readiness determines what AI can see and use; governance determines how it can operate; and explainability determines whether its outputs can be understood, challenged and defended.

Scaling AI responsibly therefore requires these capabilities to develop alongside adoption rather than after it.

5. The destination is a different operating model – not a faster version of today's

The research points toward a significant evolution in the financial crime operating model.

Today, most institutions remain dependent on hybrid models combining manual processes, rules and automation. Looking ahead, 73.5% expect their financial crime compliance function to operate through either a hybrid model, with AI supporting human-led processes (44.4%), or an AI-augmented model, where AI handles most tasks and humans provide oversight (29.1%). Only 10.3% anticipate a highly autonomous model.

But the future model is not defined by automation alone.

The gap between today's operating reality and that future model is particularly visible in continuous monitoring. Just 4.7% of respondents say the majority of their monitoring and controls operate continuously, while 56.8% have not adopted always-on compliance monitoring, are only exploring it or remain at an early pilot stage.

When respondents were asked what will characterize a high-performing next-generation financial crime function, no single capability dominated. Real-time monitoring, efficiency, governance and explainability, measurable compliance effectiveness, adaptability and AI-driven decision-making all rank within a narrow range, indicating that high performance will depend on these capabilities working together.

That means moving beyond the application of AI within individual silos toward operating models in which data, risk intelligence, detection, investigation, governance and decision-making are increasingly connected. AI can enable that transition, but technology alone does not constitute transformation.

What this means for financial crime leaders

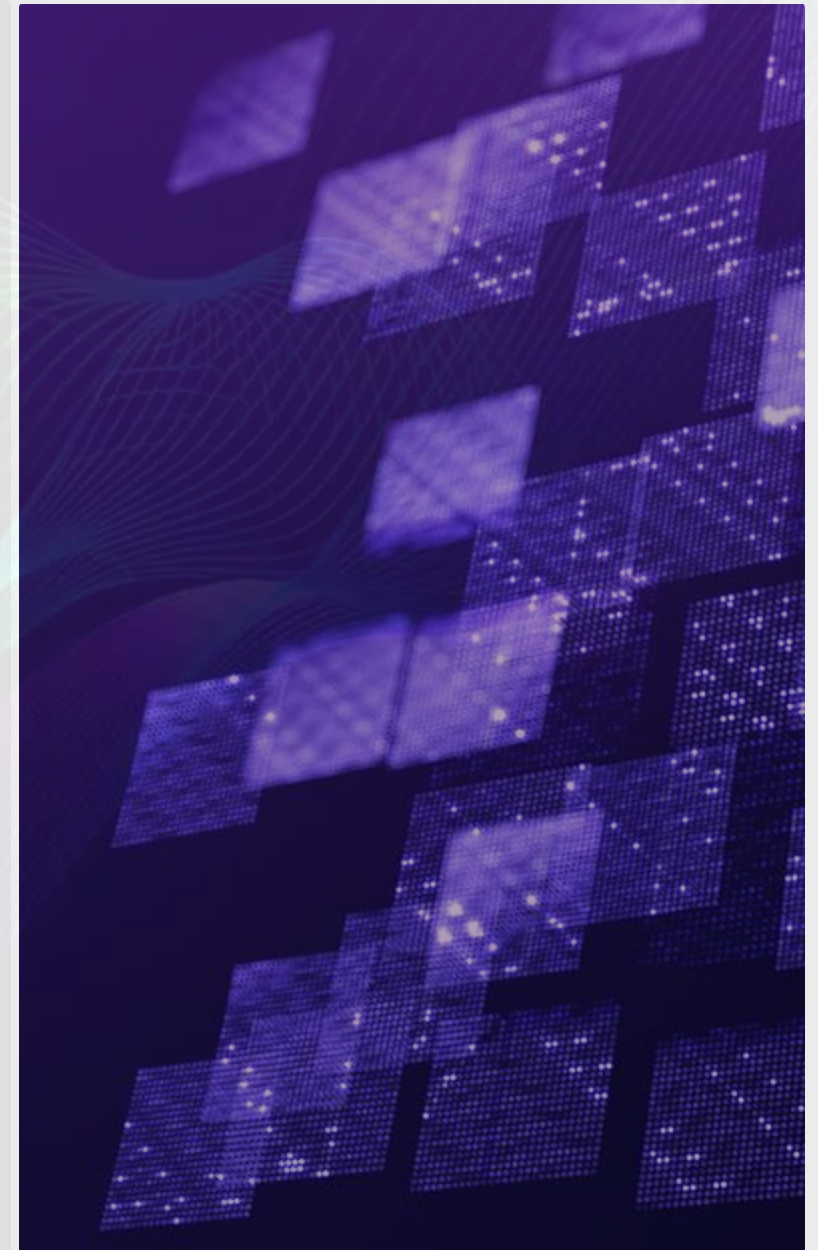
Taken together, the findings point to a shift from AI adoption toward accountable impact. The question is no longer simply where AI can be deployed, but

whether institutions have the data, governance, technology, skills and operating model required to translate innovation into measurable improvements in financial crime compliance.

Effectiveness, efficiency and explainability provide the critical tests. AI-enabled controls must improve the identification and management of risk; automation must reduce unnecessary activity and focus expertise where it creates the greatest value; and increasingly AI-enabled decisions must remain understandable, governable and defensible.

The research does not point toward technology replacing financial crime expertise or accountability. It points toward a more connected, adaptive and increasingly always-on financial crime function in which AI takes on a greater share of operational activity while human judgment and accountability remain central.

As financial crime operating models evolve, progress will be measured not by AI adoption itself, but by whether it delivers more effective, efficient and explainable financial crime compliance.



Methodology and respondent profile

FinCrime Frontier is an annual industry study examining how financial institutions are responding to the evolving regulatory, operational, and technology landscape in financial crime compliance. The 2026–27 study provides a current view of industry priorities, challenges and investment decisions, while tracking how financial crime compliance is evolving year over year.

Conducted jointly by SymphonyAI and AML Intelligence, the 2026–27 survey gathered responses from 202 financial crime, compliance, risk, operations, technology and executive professionals across financial services organizations in EMEA and the Americas.

The survey was conducted online between June 2 and July 10, 2026, and comprised 30 structured questions. Questions covered seven areas: the financial crime market landscape; regulatory developments and challenges; the economics of compliance; operational efficiency and effectiveness;

AI and automation maturity; AI governance and data readiness; and innovation and the future outlook.

The respondent base spans banking, payments and fintech, insurance, digital assets and other financial services organizations, and includes institutions of different sizes and geographic markets. Compliance and financial crime professionals represent the largest share of respondents, complemented by perspectives from risk, operations, technology, data and AI, and executive leadership.

The findings are based on respondents' reported experiences, priorities and expectations and should be interpreted as indicators of industry direction rather than as a statistically representative measure of the global financial services market. Where questions permitted multiple responses, percentages may total more than 100%. Where relevant and sufficiently comparable, findings from the 2026–27 study are considered alongside results from the previous FinCrime Frontier survey to identify changes in industry priorities and maturity.

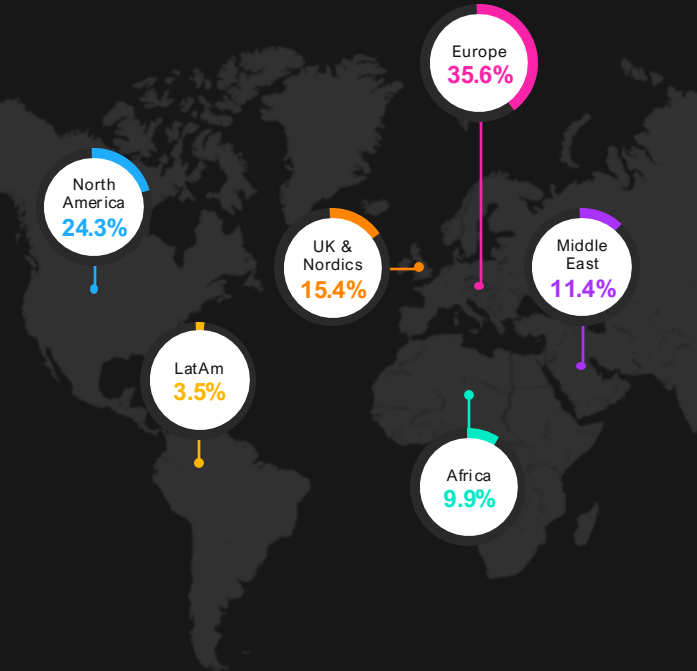
Together, the findings provide an evidence-based view of how financial crime compliance is evolving – from regulatory and cost pressures to operational performance, AI adoption and the transition toward more intelligent, adaptive and continuously operating compliance models.

202 financial crime and compliance professionals across EMEA and the Americas, with 62% of respondents at Senior Manager level or above, including 44% at Head/Director or C-suite/Executive level.

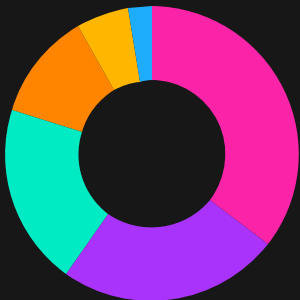
2026–27 respondent profile

202 respondents

Geographic reach

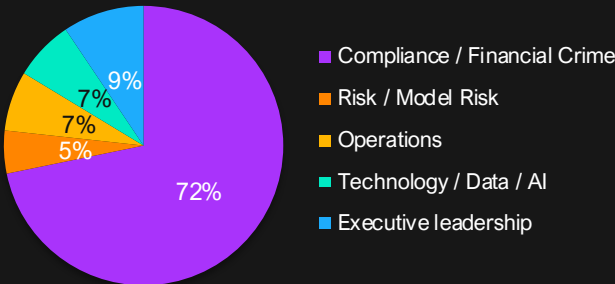


Organization type

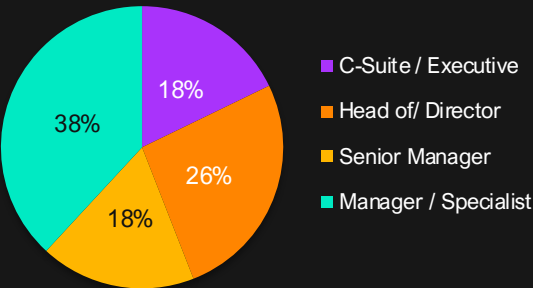


- 24.3% Retail banking
- 11.9% Corporate / investment banking
- 5.9% Insurance
- 19.8% Payments / fintech
- 2.5% Crypto / digital assets
- 35.6% Other financial services

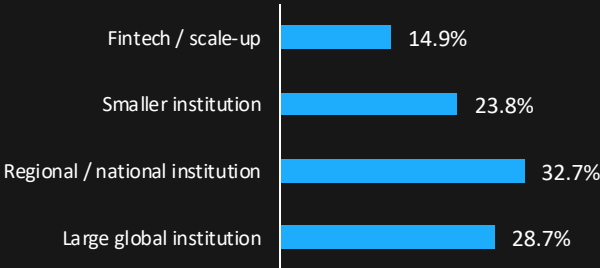
Primary roles



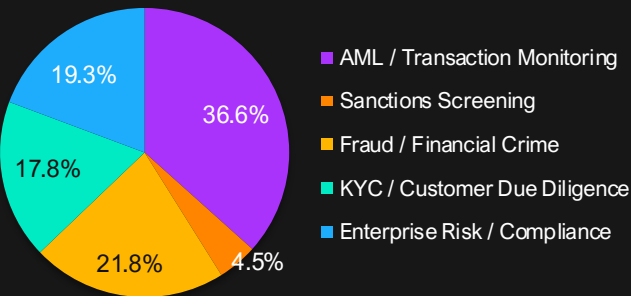
Seniority



Organization size



Primary focus area



The new financial crime landscape

Threats and operating models are evolving

Traditionally financial crime compliance processes and systems were built using a retrospective approach: assess risk, develop then calibrate controls, generate alerts and periodically revisit those controls as risks changes. That model is increasingly being challenged by a threat environment that is faster-moving, more interconnected and increasingly technology-enabled.

Additionally, the risk-based approach (RBA) was never intended to be a static exercise, but in practice periodic risk assessment and control calibration often struggle to keep pace with a fast-changing threat environment. The result is a widening gap between how financial institutions are organized to detect and prevent financial crime and how it is actually being committed.

A more dynamic approach is needed one that uses current data and threat intelligence to continuously inform risk assessment, scenario coverage and control calibration. Internal intelligence, investigative outcomes, external threat intelligence / industry insights and law enforcement information where available, informs such programs, helping controls adjust as the threat environment changes.

The findings point to a continuing shift toward greater use of data, automation and real-time capabilities, although most institutions remain some distance from predictive, proactive financial crime management. Persistent gaps in data, processes and technology continue to constrain institutions' ability to respond at the speed of the threat.

1.1 Financial crime detection operating models are undergoing structural transformation

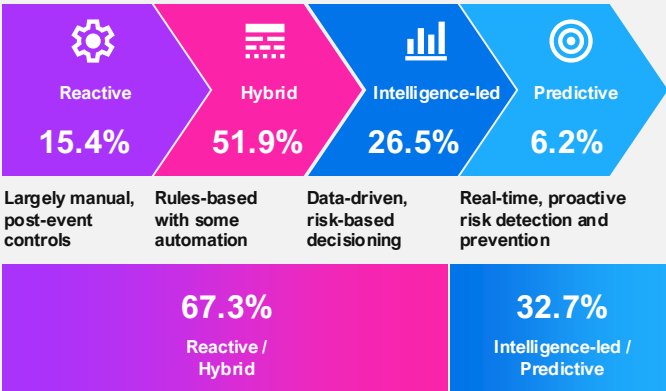
Financial crime detection operating models are evolving, but most institutions remain in the middle of the transition.

More than half of respondents (51.9%) describe their current model as hybrid, combining rules-based

controls with some automation. A further 15.4% remain largely reactive, relying on manual, post-event controls.

By contrast, 26.5% describe their operating model as intelligence-led, using data to support risk-based decision-making, while just 6.2% report having reached a predictive model built around real-time, proactive risk detection and prevention.

Financial crime operating model maturity



Two-thirds of respondents (67.3%) still operate reactive or hybrid financial crime operating models. Only 32.7% describe their organizations as intelligence-led or predictive.

The distribution reflects an industry that has begun to modernize its controls, but where more advanced,

intelligence-led and predictive operating models remain relatively limited. Moving toward more intelligence-led operations will require institutions to make greater use of customer, transaction, investigative and external intelligence in detection and decision-making, enabling controls to respond more dynamically as risks change.

Last year's findings already pointed to this transition. In the 2025–26 survey, 61% of respondents described alert review as partially automated with human review, while only 2.4% reported fully automated processes. Although the measures are not directly comparable, the findings provide useful context: institutions have been introducing automation, but the broader transition from reactive controls toward proactive financial crime management remains incomplete.

The small proportion of organizations already operating predictively also highlights the scale of that transition. Moving from hybrid to intelligence-led and ultimately predictive operations requires institutions to strengthen the foundations that enable more timely risk detection and decision-making, particularly data integration, technology and analytics, real-time capabilities and effective collaboration. As the following sections show, these remain some of the industry's most persistent capability gaps.

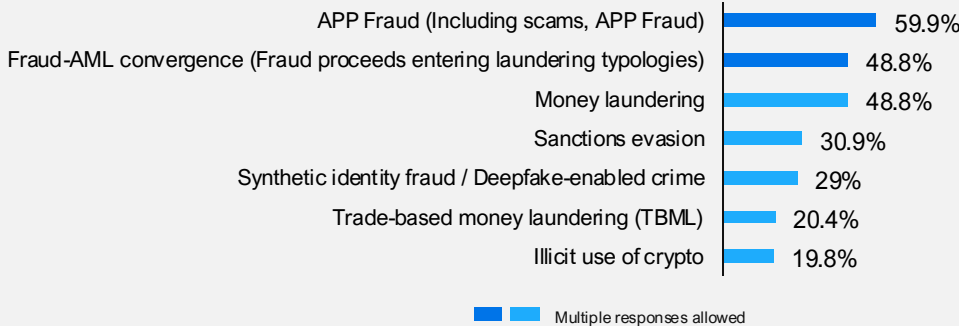
1.2 Financial crime risks are increasingly converging

Fraud ranks as the financial crime risk increasing most in importance, cited by 59.9% of respondents. Almost half (48.8%) also identify fraud–AML convergence – where the proceeds of fraud enter money laundering typologies – while the same proportion cite money laundering itself.

Other threats add further complexity. Sanctions evasion is increasing in importance for 30.9% of respondents, while 29% identify synthetic identity fraud and deepfake-enabled crime. Trade-based money laundering (20.4%) and the illicit use of crypto (19.8%) rank lower but remain significant elements of a threat landscape increasingly shaped by digital channels, cross-border activity and new methods of concealment.

The findings reflect an environment in which fraud and money laundering are increasingly difficult to address as separate problems. Fraud generates illicit proceeds that must be moved, concealed or integrated into the financial system, while the same customers, accounts, networks and transaction flows can span multiple forms of financial crime. Criminal activity does not conform to the organizational boundaries between fraud, AML, sanctions and KYC, highlighting the value of sharing relevant intelligence across financial crime disciplines.

Financial crime risks increasing most in importance



Threat landscape in focus

Several shifts are reshaping the current threat landscape:

Convergence across fraud, AML, sanctions, and KYC.

Criminal activity does not conform neatly to traditional financial crime categories. Account takeover, APP fraud and money mule networks can generate signals relevant across multiple areas of financial crime, increasing the importance of sharing relevant risk intelligence across disciplines.

Sanctions complexity.

Faster-moving regimes and evolving evasion techniques – including shell structures, trade-based evasion and third-country routing – challenge screening approaches built primarily around static list matching.

Crypto and digital assets.

As traditional and digital payment rails converge, exposure to crypto-related financial crime risk can extend beyond institutions directly servicing digital assets.

AI-enabled synthetic identity and deepfakes.

Synthetic identities, voice cloning, synthetic documents and AI-generated identity artifacts are increasing pressure on traditional identity verification and rules-based detection.

The survey findings mirror a broader shift in the international response to financial crime. [FATF's 2026–2028 Roadmap](#) on Combatting Fraud places fraud among its strategic priorities and calls for stronger financial intelligence, cross-sector collaboration and international cooperation.

FATF has also called for the AML/CFT/CPF toolkit to be deployed more fully against fraud, while emphasizing stronger public-private, cross-border and private-to-private information sharing. The direction is significant: fraud can no longer be treated solely as a discrete loss-prevention problem, separate from the wider financial crime ecosystem.

For financial crime leaders, the implication is that controls designed around individual risk categories may increasingly struggle to capture how threats interact in practice. Bringing together relevant customer, transaction, behavioral and external risk information can provide a broader view of suspicious activity and help institutions identify relationships across different forms of financial crime.

1.3 The biggest constraint is execution

As financial crime risks become more interconnected, institutions need the ability to turn data and intelligence into timely action.

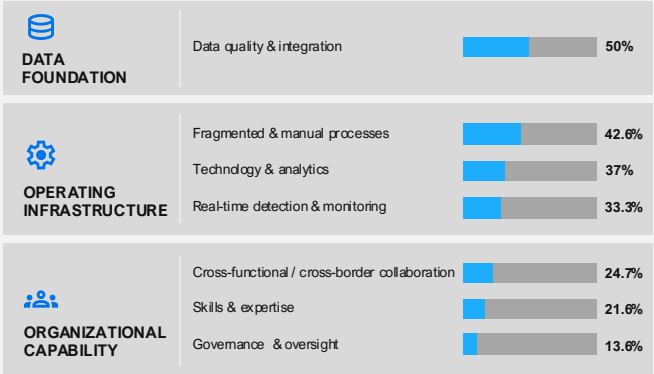
The survey points to a combination of data, process, technology and organizational constraints affecting institutions' ability to manage emerging financial crime risks. These challenges are interconnected and can limit how quickly institutions translate changing risk into effective detection and response.

The survey shows where the most significant gaps lie.

Data quality and integration is the most widely cited gap, identified by 50% of respondents. Fragmented and manual processes follow at 42.6%, while 37% point to limitations in technology and analytics capability.

A further 33.3% identify real-time detection and monitoring as a gap.

The execution gap spans data, infrastructure and organizational capability



Respondents could select up to three answers.

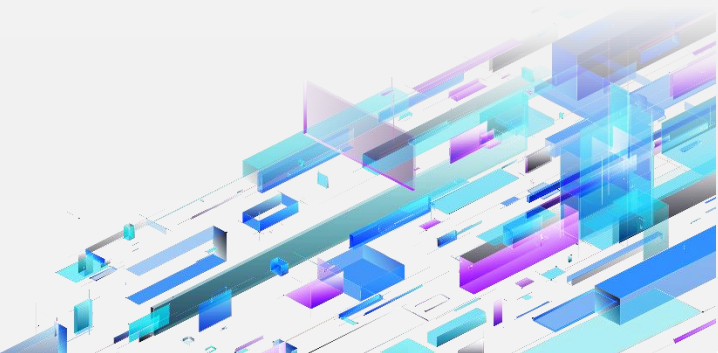
The pattern is significant because these capabilities are closely connected. Fragmented data limits the effectiveness of analytics; disconnected and manual processes slow the movement of intelligence into investigations and decisions; and technology constraints make it harder to detect changing patterns of risk in real time.

The findings also point to the persistence of challenges identified in last year's survey. In 2025–26, data quality and integration was the leading operational pain point, cited by 65.6% of respondents, while outdated or inadequate technology was identified by 39.5%. A separate assessment of technology limitations

highlighted legacy integration, siloed data and limited real-time capabilities among the principal constraints. While the questions are not directly comparable year-over-year, the direction is consistent: data, integration and technology remain structural challenges for financial crime operations.

Organizational factors rank lower but remain important. Cross-functional and cross-border collaboration is identified as a gap by 24.7% of respondents, followed by skills and expertise at 21.6% and governance and oversight frameworks at 13.6%. Together, the findings show that execution challenges extend beyond technology to the organizational capabilities required to respond effectively to changing financial crime risks.

The challenge for financial crime leaders is therefore one of execution. Progress will depend on strengthening data, processes, analytics and real-time capabilities so that institutions can respond more effectively as financial crime risks evolve.



What this means for financial crime leaders

The findings point to a mismatch between the financial crime threat environment and the operating models designed to manage it. Risks are becoming more interconnected and fast-moving, yet most institutions remain reliant on hybrid or reactive approaches, while persistent gaps in data, processes and technology constrain their ability to respond in real time.

Three takeaways

- 1 OPERATING MODELS ARE IN TRANSITION**
Hybrid models dominate, but relatively few institutions have progressed to intelligence-led or predictive operations.
- 2 THREATS ARE CONVERGING**
Fraud, money laundering and fraud-AML convergence increasingly form part of an interconnected risk landscape, challenging traditional functional boundaries.
- 3 EXECUTION IS THE CONSTRAINT**
Data quality and integration, fragmented processes, technology and real-time detection remain the principal gaps between current capabilities and more proactive financial crime management.

The direction of travel is clear: financial crime compliance is moving toward greater use of data, automation, intelligence and real-time capabilities. Achieving that transition will depend on how effectively institutions address persistent gaps in data, processes, technology and organizational capability while maintaining a clear focus on the effectiveness of financial crime risk management.

From regulatory change to regulatory adaptability

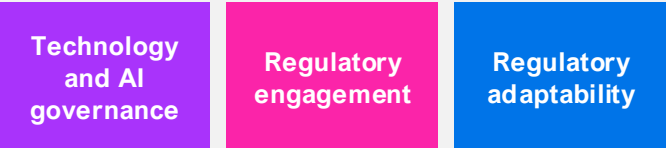
The regulatory environment for financial crime compliance is entering one of its most consequential phases in over a decade. Regulators across the EU, UK and US are simultaneously expanding expectations, demanding greater transparency, stronger governance, and demonstrable effectiveness from the technology that underpins FinCrime compliance programs.

The survey findings show that AI and model governance expectations and regulatory expectations around technology and system adequacy jointly rank as the foremost regulatory challenge facing compliance functions today, each cited by 40.8% of respondents. This underscores a defining shift: regulators are no longer evaluating whether firms have a policy – they are evaluating whether the technology behind it performs as expected and can

be evidenced.

Data integrity, jurisdictional alignment, and the pace of regulatory change are the defining themes shaping 2026–27 compliance strategies. Yet the central tension lies not in intent, but in execution: how organizations respond to these pressures and how mature their relationship with regulators has become, will determine who leads the next compliance cycle and who falls behind it.

Key themes

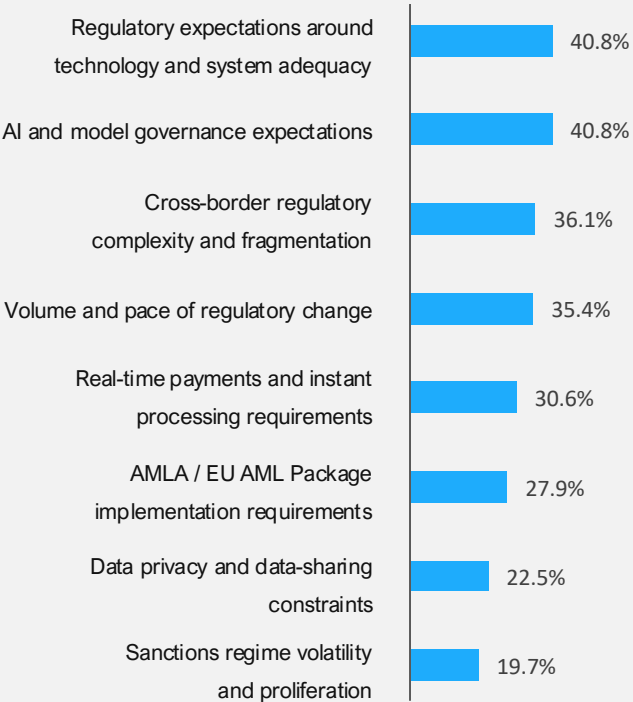


2.1 Regulatory priorities shaping technology investment

AI and model governance expectations and technology/system adequacy jointly rank as the leading regulatory challenges, each cited by 40.8% of respondents. Cross-border regulatory complexity (36.1%) and the volume and pace of regulatory change (35.4%) confirm what practitioners are experiencing directly: the pipeline is moving faster than most functions can absorb, and it is not moving consistently

across jurisdictions. An institution operating across the EU, UK and US simultaneously absorbs regulations such as the AMLA AMLR's directly-applicable Single Rulebook, the FCA's enforcement expectations, and FinCEN's BSA modernization program – frameworks that share objectives but diverge on specifics.

Most significant regulatory challenges impacting compliance functions



Multiple responses allowed

AMLA and EU AML Package implementation requirements (27.9%) and real-time payments (30.6%) reflect the infrastructure investment that regulatory convergence now demands. Sanctions regime volatility (19.7%) and data privacy constraints (22.5%) sit lower by frequency but represent pressure points that will intensify as supervisory perimeters expand into new sectors and geographies.

A significant shift from 2025–26

In the prior year's survey, navigating the patchwork of global AML regulations was the dominant concern, cited by nearly 57% of respondents – a clear indication that regulatory fragmentation was straining multinational compliance programs. In 2026–27, that figure has receded to 36%, with AI governance and technology adequacy rising jointly to claim the top position. The industry has internalized cross-border complexity as a structural constant. Regulatory scrutiny has moved upstream to whether the technology used to navigate that complexity is itself fit for purpose.

Recent developments reinforce that direction. FinCEN's proposed AML/CFT program modernization reforms and the FCA's scrutiny of sanctions systems and controls point toward greater emphasis on whether financial crime programs remain risk-based.

The investment implication is direct. Platforms that cannot produce structured, auditable, traceable outputs are not simply operationally inefficient, they are becoming supervisory liabilities. Across all three markets, the regulatory direction is identical: demonstrate that your technology works, not just that it exists.

2.2 From compliance to transformation

Regulatory change is being experienced as 'increased workload' before it is experienced as 'transformation'. More than a quarter of respondents (26.5%) say regulatory change is forcing reactive changes and increased workload. A further 15.7% characterize it as driving only incremental improvements. Together, more than four in ten are absorbing regulatory change as operational pressure rather than strategic opportunity.

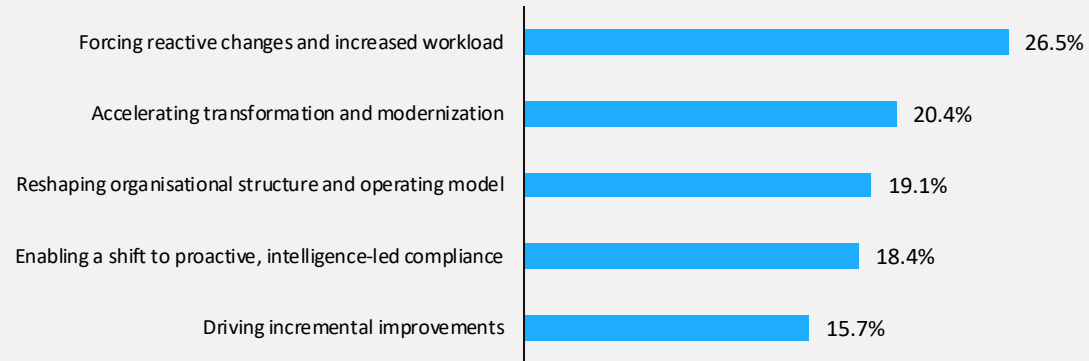
The forward-leaning cohort is meaningful but not yet dominant. 20.4% say regulation is accelerating transformation and modernization; 19.1% report it is reshaping their organisational structure and operating model; and 18.4% describe it as enabling a shift to proactive, intelligence-led compliance. In aggregate, some 58% describe a forward-leaning response – but the single largest individual category remains reactive.

Regulatory change remains an operational burden, but for most it is also becoming a catalyst for change.

By comparison, in 2025–26, a clear majority (58%) viewed upcoming regulation as a positive catalyst for modernization, with only 14% foreseeing negative consequences. That sentiment broadly holds in 2026–27. What has changed is the granularity: when asked how regulation is influencing strategy in practice today, more than a quarter still describe it as reactive workload. The challenge lies not in intent, but in execution.



Regulatory change is driving strategic change, but reactive responses still lead



Organizations absorbing regulation reactively – updating rule sets, workflows, extending screening as new obligations emerge – risk adding complexity without building underlying capability. By contrast, firms using regulatory change as a catalyst for transformation can build more adaptable data, technology and control architectures that support multiple requirements and reduce the need for repeated, requirement-by-requirement remediation.

The challenge for compliance leaders is therefore not simply to interpret regulatory change, but to build the capability to operationalize it consistently and at pace across real-time, data-driven, cross-border ecosystems.

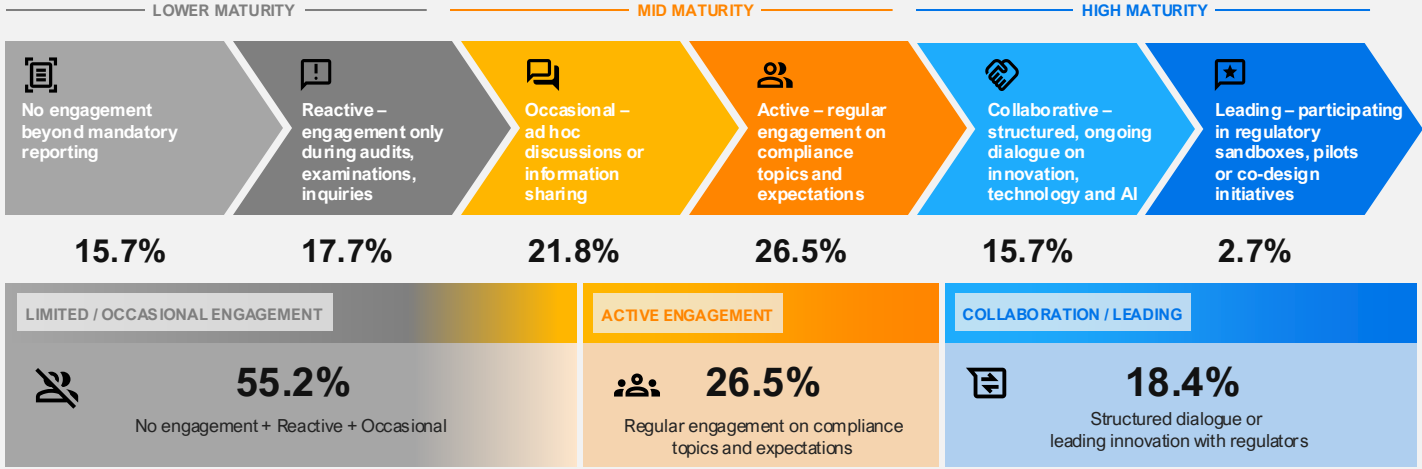


2.3

The changing regulator relationship

Regulator engagement on compliance technology and AI remains limited and largely ad hoc. While 26.5% of organizations report active, regular engagement – the largest single category – a combined 33.4% have no meaningful dialogue with their regulator outside mandatory reporting and examination responses. The collaborative tier, where structured ongoing dialogue on technology and innovation takes place, accounts for just 15.7%. Only 2.7% are participating in regulatory sandboxes, pilots or co-design initiatives.

Engagement maturity spectrum



These findings confirm that most regulatory engagement remains reactive and clarification-driven rather than collaborative. The frequency, depth and quality of engagement with regulators remains uneven, indicating a clear need for more proactive, technology-informed dialogue between compliance leaders and supervisory bodies.

From clarification to collaboration: the evolving regulator-institution dialogue

2025: Regulatory engagement was relatively common, but largely centered on clarification and compliance maintenance.

2026–27: Regular engagement is becoming more established, but deep collaboration on technology and AI remains the exception rather than the norm.

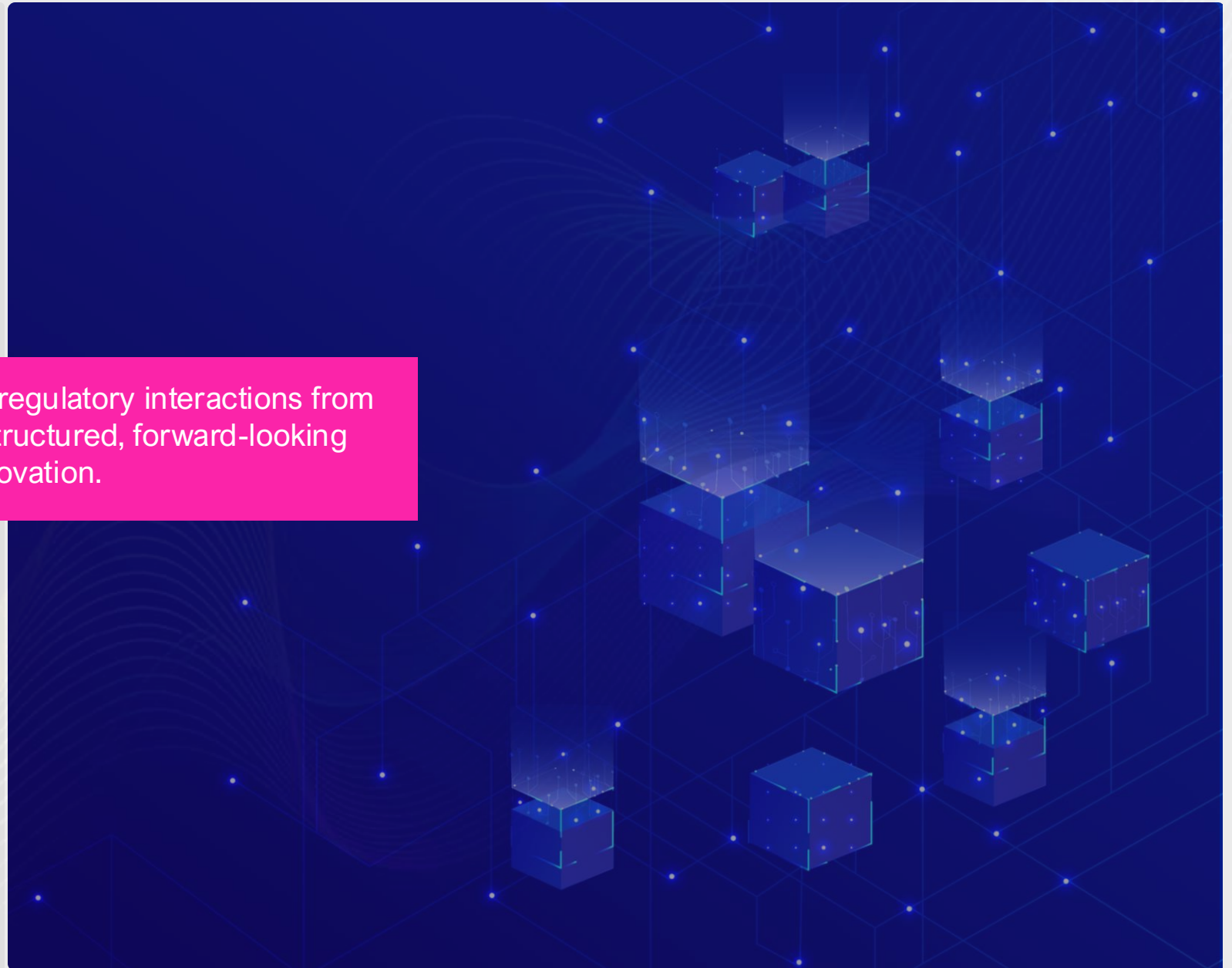
Regulators across all three markets are deploying advanced analytics to form views of firm-level risk between examination cycles. Organizations in the active and collaborative tiers are operating in a materially different supervisory relationship – one shaped by proactive engagement. Those remaining reactive are responding to a narrative their regulators has already formed without them.

The next frontier lies in transforming regulatory interactions from periodic compliance check-ins into structured, forward-looking conversations on technology and innovation.

2.4

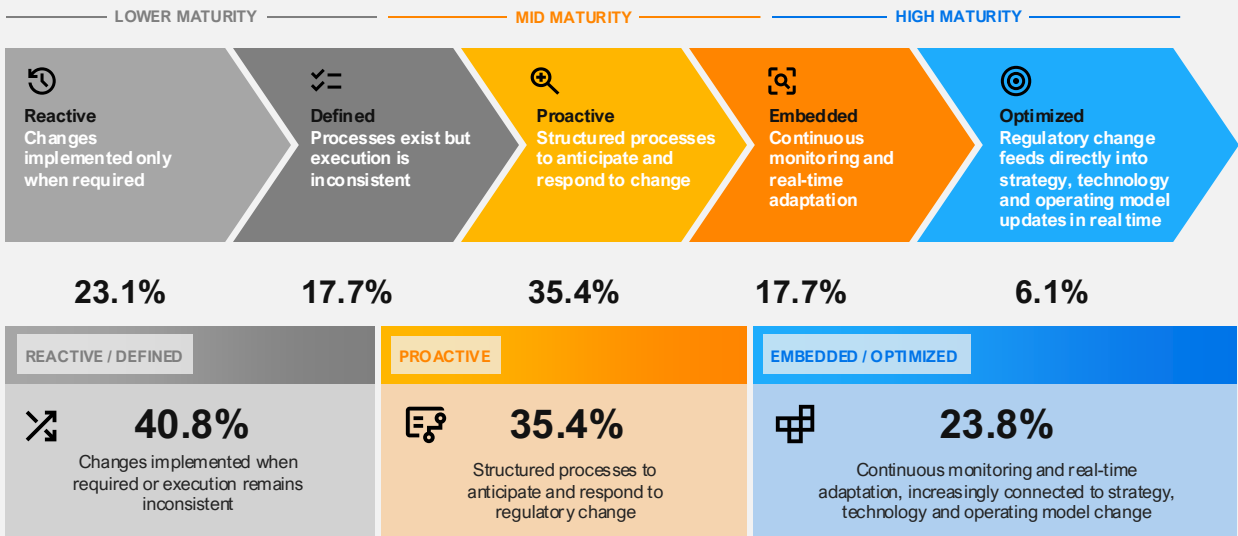
Regulatory readiness as a strategic capability

Numerous organizations (35.4%) operate with a proactive capability: structured processes to anticipate and respond to regulatory change before it arrives. The sector's operational baseline is proactive, but not yet the industry baseline. 40.8% remain reactive or defined-but-inconsistent in their execution, and only 23.8% describe their capabilities as embedded or optimized, with continuous monitoring, real-time



adaptation or direct integration into strategy, technology and operating-model decisions. Just 6.1% operate at the optimized level, where regulatory change feeds continuously into strategy, technology and operating model decisions.

Regulatory change maturity spectrum



These findings confirm that most regulatory engagement remains reactive and clarification-driven rather than collaborative. The frequency, depth and quality of engagement with regulators remains uneven, indicating a clear need for more proactive, technology-informed dialogue between compliance leaders and supervisory bodies.

Positive intent does not equal operational readiness

Last year's finding showed 58% viewed regulation positively as a modernization driver, however this is contrast to the 2026–27 finding where 41% describe their operationalization capability as 'reactive' or 'inconsistent'. Regulatory sentiment and regulatory readiness are not the same thing. And that gap is now measurable for the first time.

Institutions at the proactive tier have horizon-scanning processes to identify and track movement and execution. What most lack is the governance architecture to translate that intelligence into technology investment decisions, capital allocation and board-level planning. The 6.1% at optimized maturity have made that step. At the highest level of maturity, this could mean treating regulatory intelligence as a shared enterprise capability, mapping emerging obligations against technology and control architectures, and incorporating regulatory change into forward investment planning.

As regulatory obligations across AML, AI governance and operational resilience continue to converge, organizations that have not yet elevated regulatory readiness to a board-level discipline will find the 2027 compliance cycle increasingly difficult to absorb. Those that have will be better positioned to compete, not just to comply.

Only 23.8% have reached a level where regulatory change is continuously monitored and translated into real-time adaptation or broader strategic and operating-model updates.

Key insights

The findings point to an industry moving from reactive regulatory implementation toward continuous adaptability, but the transition remains incomplete. Technology expectations are rising, regulatory collaboration remains limited, and only a minority of firms have embedded regulatory change into continuously adaptive operating models.

Technology adequacy is the new supervisory frontier.	The execution gap is now visible.	One third of the market is invisible to its regulator.	Proactive is not enough	Early regulatory dialogue can reduce implementation uncertainty.
AI governance and technology system adequacy jointly top the regulatory challenge list at 40.8% each – up sharply from cross-border complexity's dominance in 2025–26. Regulators are no longer auditing policy. They are auditing performance.	58% expressed positive regulatory sentiment in 2025–26. In 2026–27, reactive workload remains the largest individual strategic response with 26.5%. Intent and readiness are diverging – and the gap is measurable.	33% engage only during mandatory reporting or examinations. In an environment where supervisors are forming views of firm-level risk between cycles using advanced analytics, that is an accumulating supervisory deficit.	Embedded is the target. Only 23.8% have reached embedded or optimized maturity. The move from proactive awareness to embedded capability – integrating regulatory intelligence into technology investment and board-level planning – is the priority transition before 2027 obligations arrive.	The 2.7% participating in regulatory co-design and sandboxes are a small but strategically significant cohort. Early dialogue with supervisors – on AI governance, data standards and cross-border interoperability – is a competitive advantage, not a compliance courtesy.

What leaders should do

- Build regulatory adaptability into the operating model.** Connect horizon scanning and regulatory intelligence more directly with control design, technology roadmaps, data requirements and operational change.
- Treat technology governance as regulatory infrastructure.** As technology adequacy and AI governance move higher on the supervisory agenda, explainability, accountability, validation and human oversight should be designed into technology adoption rather than added retrospectively.
- Move regulatory engagement upstream.** Where appropriate, engage regulators earlier around emerging technologies, implementation questions and governance approaches rather than relying predominantly on examination- or inquiry-driven dialogue.
- Design for reusable change.** Reduce the cost and disruption of successive regulatory requirements by investing in adaptable data, technology and control architectures rather than solving each regulatory change independently.
- Measure the transition from reactive to adaptive compliance.** Track not only whether regulatory changes are delivered on time, but how quickly regulatory intelligence translates into changes to controls, technology and operations.

The economics of compliance

Cost pressures in financial crime compliance remain substantial, with technology and people continuing to dominate the cost base. At the same time, compliance leaders are under growing pressure to improve effectiveness while managing expenditure and responding to regulatory change, technology modernization and increasingly complex financial crime risks.

The investment response is becoming clearer. Organizations are directing capital toward AI, automation and the data foundations needed to support them, with the expectation that these capabilities will reduce manual work and improve the productivity of core compliance processes.

Yet investment ambition is running ahead of measurement discipline. More than half of organizations still have no formal or only ad hoc approach to measuring technology ROI, while relatively few track the unit economics of compliance. The challenge is therefore shifting from simply controlling compliance costs to demonstrating that

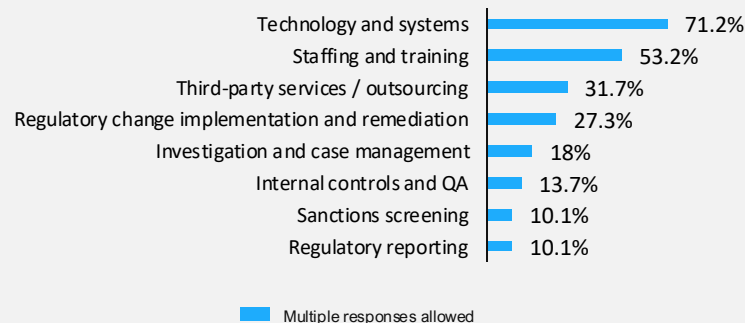
technology investment translates into measurable improvements in efficiency, effectiveness and risk outcomes.

3.1 Technology and people continue to dominate the cost base

The cost landscape for financial crime compliance remains dominated by technology infrastructure and staffing.

When asked to identify the areas driving the highest compliance costs today, 71.2% of respondents selected technology and systems, making it the dominant source of cost pressure. Staffing and training follows at 53.2%, while third-party services and outsourcing ranks a distant third at 31.7%.

Top drivers of compliance costs



Regulatory change implementation and remediation is cited by 27.3%, followed by investigation and case management at 18%. More discrete compliance activities – including internal controls and QA (13.7%), sanctions screening (10.1%) and regulatory reporting (10.1%) – are less frequently identified among organizations' three highest cost drivers.

The findings broadly reinforce the 2025–26 FinCrime Frontier survey, where technology investment, and staffing and training were also the two highest-ranked areas of cost impact. Together, they accounted for 66.1% of respondents' first-ranked cost pressures. While the methodologies differ and the percentages are not directly comparable, the consistency of the ranking is notable: the fundamental economics of compliance remain shaped by the combined cost of technology and human expertise.

Financial institutions therefore face a difficult investment equation. Modernization requires continued spending on systems, infrastructure and data, while complex investigations, governance and regulatory decision-making continue to depend heavily on skilled people.

Attention is therefore shifting from managing existing cost pressures to investing in capabilities that can change the economics of compliance.

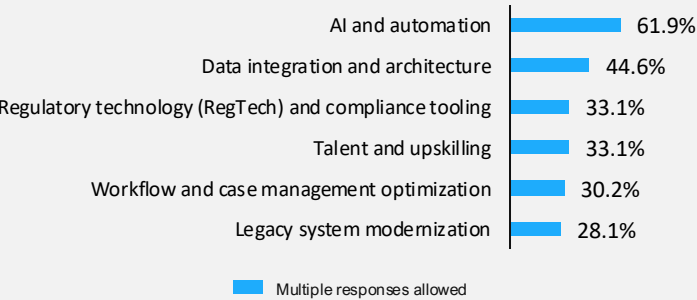
3.2
Investment is shifting toward AI
and its foundations

Where organizations intend to invest over the next 12–18 months provides a clear indication of how they plan to respond.

AI and automation is the leading compliance investment priority, selected by 61.9% of respondents. Data integration and architecture ranks second at 44.6%, followed by talent and upskilling and RegTech and compliance tooling, both at 33.1%.

Workflow and case management optimization is prioritized by 30.2%, while legacy system modernization ranks lowest at 28.1%.

Top compliance investment priorities
over the next 12-18 months



The combination of AI and data at the top of the investment agenda is significant. It suggests that organizations are not focusing solely on acquiring new AI capabilities; many are also directing investment toward the data foundations required to deploy them effectively.

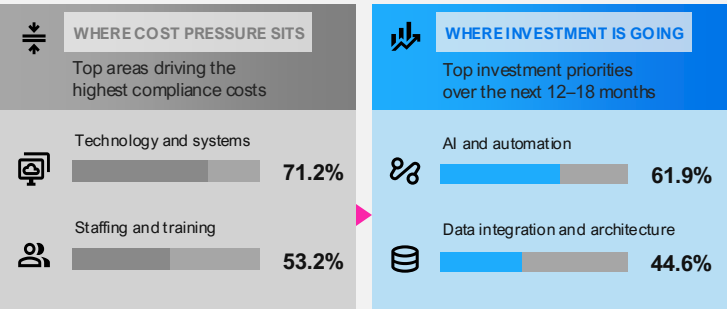
The results also provide useful continuity with the previous survey. In 2025, 45% of respondents planned to augment their existing technology stack with innovations such as AI agents, compared with 27.8% planning a rip-and-replace approach. Upskilling existing employees was selected by 56.8%, while 44.4% planned to recruit specialist financial crime, data science and analytics talent.

The questions are not directly comparable, but together they point toward an evolving investment strategy: institutions are continuing to build human capability while placing greater emphasis on technology-enabled productivity.

Legacy modernization remaining at 28.1% is also notable. It does not necessarily mean organizations are neglecting legacy technology – AI, data and workflow investments may themselves form part of wider modernization programs. But the investment hierarchy suggests that institutions are placing greater emphasis on adding intelligence, automation and connectivity than on wholesale system replacement.

The investment agenda is shifting from supporting existing compliance processes toward changing how compliance work is performed. AI and automation offer the potential to absorb repetitive work, improve prioritization and allow skilled teams to concentrate on higher-value risk decisions.

From maintaining compliance capacity to
improving compliance productivity



Note: Results are drawn from separate survey questions and illustrate the relationship between current cost pressures and future investment priorities; percentages are not directly comparable.

AI investment is accelerating. The leadership challenge is now how to convert that investment into measurable value.

3.3

Investment ambition is running ahead of ROI discipline

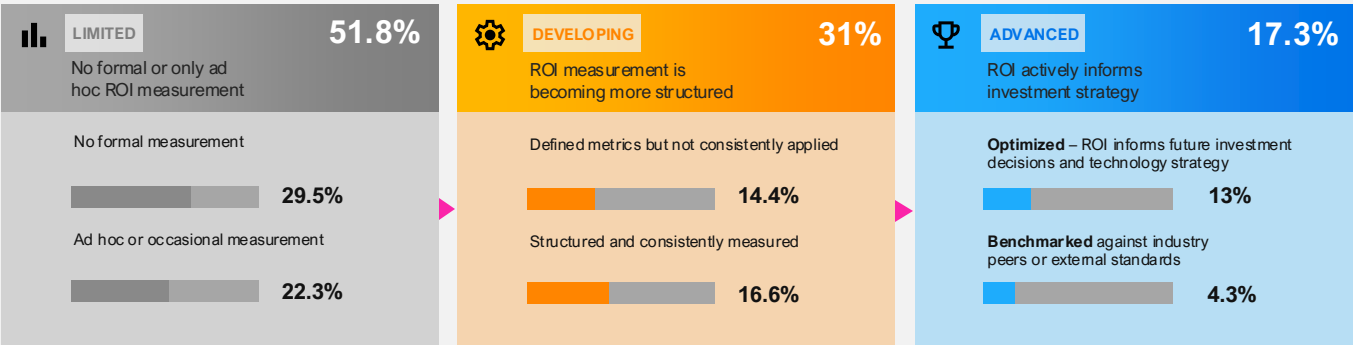
As technology investment accelerates, the ability to demonstrate its economic value remains considerably less mature.

Nearly three in ten organizations (29.5%) have no formal approach to measuring ROI on compliance technology investments, while a further 22.3% measure ROI only on an ad hoc or occasional basis.

Another 14.4% have defined metrics but do not apply them consistently. Only 16.6% report structured and consistent measurement, while 13% have reached the point where ROI measurement informs future investment decisions and technology strategy. Just 4.3% benchmark performance against industry peers or external standards.

Put another way, 51.8% of organizations have no formal or only ad hoc ROI measurement, rising to 66.2% when organizations with defined but inconsistently applied metrics are included.

ROI discipline is lagging investment ambition



Note: Percentages may not total 100% due to rounding.



More than half of organizations (51.8%) have no formal or only ad hoc approach to measuring ROI on compliance technology investments.

The previous survey provides useful context. While the questions are not directly comparable, the results indicate that systematic ROI discipline remains underdeveloped across much of the industry. In 2025, 71.9% of respondents said they had not conducted an ROI analysis on their compliance technology investments, while 28.1% had.

That creates an important tension at the center of the compliance investment agenda. AI and automation is now the No. 1 investment priority, yet more than half of organizations lack a systematic approach to determining whether technology investments are delivering value.

As AI programs move from experimentation toward broader implementation, business cases will increasingly need to demonstrate more than regulatory necessity or technical capability.

Compliance leaders will need to show measurable improvements in productivity, risk coverage and compliance outcomes, and use those results to inform subsequent investment decisions.

3.4

The measurement gap extends beyond ROI

The way organizations measure compliance performance helps explain the ROI gap.

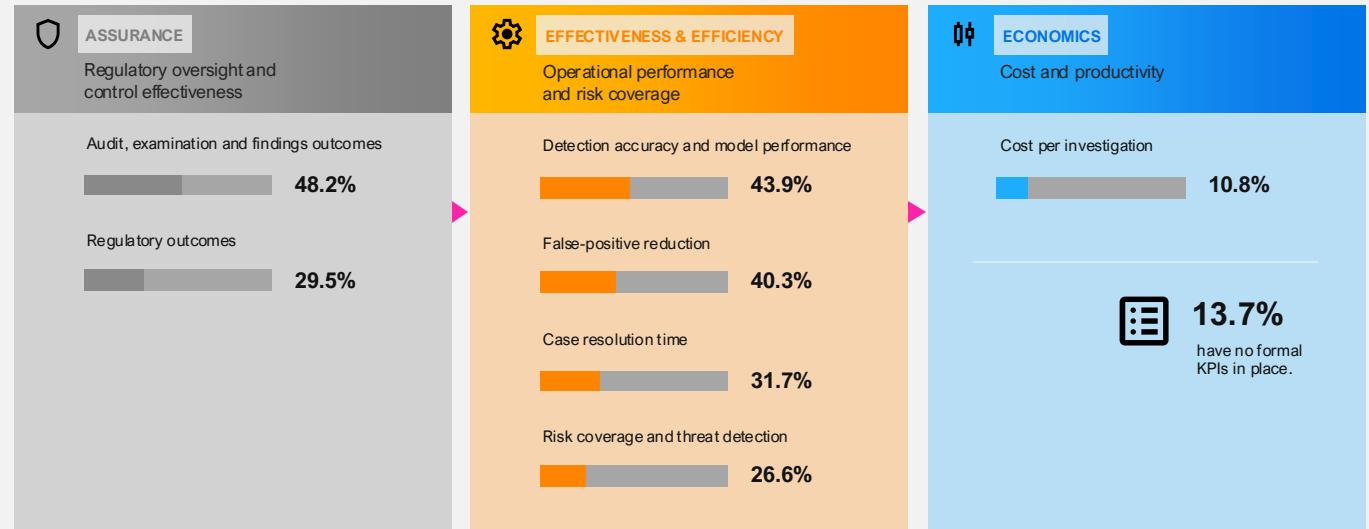
Audit, examination and findings outcomes are the most widely used KPI, cited by 48.2% of respondents. Detection accuracy and model performance follows at 43.9%, with false-positive reduction at 40.3%.

Operational measures also feature prominently. Case resolution time is tracked by 31.7%, regulatory outcomes such as SAR quality by 29.5%, and risk coverage and threat detection by 26.6%.

But explicitly financial measures are much less common. Only 10.8% identify cost per investigation among their primary compliance effectiveness KPIs, while 13.7% report having no formal KPIs at all.

What compliance functions measure

Most organizations focus on regulatory outcomes and operational performance, while fewer measure the economics of compliance.



Note: Respondents could select up to three answers.



Compliance functions are measuring assurance and operational performance, but relatively few are explicitly tracking the economics of compliance.

The contrast is revealing. Compliance functions are measuring regulatory assurance, detection performance and operational efficiency, but relatively few are explicitly connecting those outcomes to the economics of the function.

This does not mean that operational KPIs have no economic value. False-positive reduction and faster case resolution can release substantial capacity,

while better detection can strengthen effectiveness. The gap lies in translating those improvements into financial and productivity measures that can demonstrate the return on technology investment.

The next stage of measurement maturity will therefore require organizations to answer two questions: Did the investment improve the compliance outcome, and what measurable value did that improvement create?

3.5

AI is expected to deliver the efficiency dividend

Despite relatively immature ROI measurement, organizations have a clear view of where they expect future efficiencies to come from.

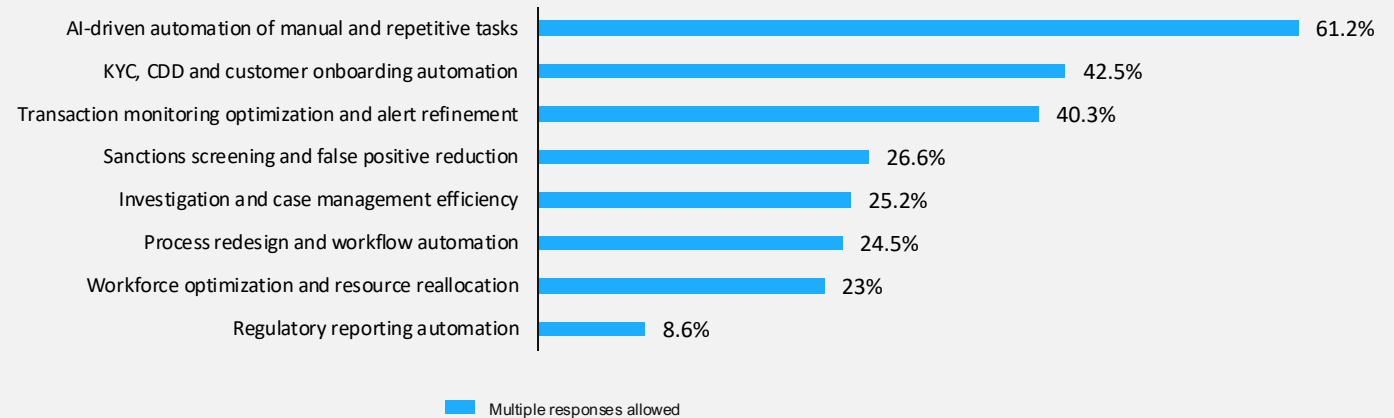
AI-driven automation of manual and repetitive tasks ranks first by a wide margin, selected by 61.2% of respondents. KYC, CDD and customer onboarding automation follows at 42.5%, while 40.3% expect significant efficiencies from transaction monitoring optimization and alert refinement.

Further opportunities include sanctions screening and false-positive reduction (26.6%), investigation and case management efficiency (25.2%), process redesign and workflow automation (24.5%), and workforce optimization and resource reallocation (23%).

Regulatory reporting automation ranks considerably lower at 8.6%.

The findings point to a practical efficiency agenda centered on high-volume, resource-intensive work. Rather than workforce optimization itself being the primary source of savings, organizations are looking first to automate repetitive activity and improve the

Top areas for cost efficiency gains over the next two years



productivity of core financial crime processes.

This difference is important. The emerging economic case for AI is not simply about reducing headcount. It is about changing the composition of compliance work: reducing manual reviews, improving alert quality, accelerating routine processes and creating capacity for human expertise to be focused on complex investigations and higher-risk decisions.

There is also strong directional continuity with the previous survey. When respondents were asked in open-ended format in 2025 where they expected future cost savings to emerge, common themes included AI and automation, transaction monitoring, sanctions screening, KYC/CDD and reduced manual effort.

Key finding: investment ambition is outpacing value measurement

AI and automation is the leading investment priority for 61.9% of organizations, and 61.2% expect AI-driven automation to deliver the greatest cost efficiencies. Yet 51.8% still have no formal or only ad hoc approach to measuring technology ROI.

From investment to measurable value

Taken together, the findings reveal a compliance investment model in transition.

Technology and staffing remain the industry's largest sources of cost, but organizations are increasingly looking to AI, automation and data to change that equation. The expected efficiency gains are concentrated in precisely the areas where financial crime operations remain highly manual and resource-intensive, including KYC/CDD, transaction monitoring, screening and investigations.

Yet the ability to prove the economic return remains a weak point. More than half of organizations have no formal or only ad hoc approach to technology ROI, while just 10.8% identify cost per investigation among their primary effectiveness KPIs.

This creates a growing imperative for compliance leaders. As investment shifts toward AI-enabled transformation, success will depend not simply on deploying technology, but on connecting investment to operational performance, operational performance to risk outcomes, and those outcomes to measurable value.

What leaders should do

Build ROI discipline into technology investment

Establish clear baselines and measurable objectives before scaling technology investments. Linking investment to productivity, risk and compliance outcomes will strengthen capital allocation and help demonstrate value.

Connect efficiency gains to compliance effectiveness

Measure automation not only by cost or time saved, but by whether it improves detection accuracy, false-positive reduction, risk coverage and regulatory outcomes. Efficiency gains should strengthen, not trade off against effectiveness.

Treat data investment as part of the AI business case

With data integration and architecture the second-highest investment priority, organizations should treat data readiness and AI as interdependent investments. The value of automation will depend on the quality, accessibility and integration of the underlying data.

Make incremental modernization deliberate

The investment pattern suggests organizations are prioritizing AI, data and workflow capabilities over wholesale legacy modernization. Leaders should ensure that incremental investment contributes to a coherent target architecture rather than adding another layer of complexity.

Use automation to redirect human expertise

The strongest efficiency opportunity lies in reducing repetitive manual work and enabling skilled teams to focus on complex investigations, judgment, oversight and higher-risk decisions. Upskilling should therefore evolve alongside technology investment.

The industry has identified its next efficiency lever. The challenge now is converting investment in AI and automation into measurable value while strengthening compliance effectiveness.

Operational performance: Closing the effectiveness gap

Financial crime functions are under growing pressure to demonstrate effectiveness through measurable outcomes and evidence of impact, rather than rely on the existence of policies, procedures and activity volumes as proxies for performance. The expectation is clear: demonstrate that controls work, and effective outcomes improve FinCrime prevention and detection. The survey suggests that while some aspects of operational performance to evidence effectiveness are improving, structural constraints in data, technology, and automation limit progress.

Alert management provides a clear example. Investigations are getting faster, but greater throughput has not yet translated into a fundamental improvement in investigative productivity. Seven in ten respondents report that no more than 5% of alerts result in escalation or SAR/STR filing, while more than a third report false-positive rates above 50%.

There are signs of progress. Nearly half of respondents now typically resolve alerts within 24 hours, and fully manual alert review has declined. Yet automation-led operating models have barely advanced year over year, leaving human investigators at the center of alert review for most institutions.

The next phase of operational improvement therefore requires a shift in emphasis: from processing more activity to improving the quality and prioritization of the activity being processed. That means addressing poor data and fragmented technology upstream, reducing low-value work before it enters the investigative funnel, and applying automation where it can free human capacity for higher-risk decisions.

The industry's early move toward Always-on Compliance points to where this evolution may lead. But with more than half of respondents still at the exploration, pilot, or pre-adoption stage, the transition from periodic controls to continuous, adaptive compliance remains a work in progress.

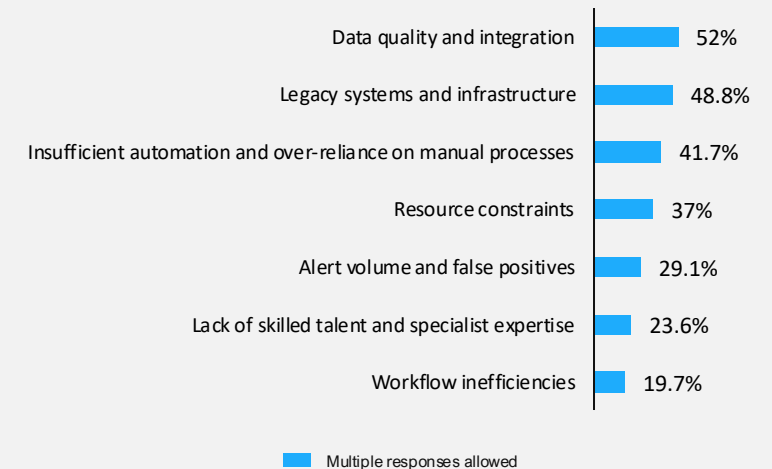


4.1

Why operational efficiency remains difficult

The operational efficiency challenge is shifting from capacity to capability. Data quality and integration remains the leading barrier at 52%, followed by legacy systems and infrastructure (48.8%) and insufficient automation and reliance on manual processes (41.7%). Resource constraints, by comparison, rank fourth at 37%.

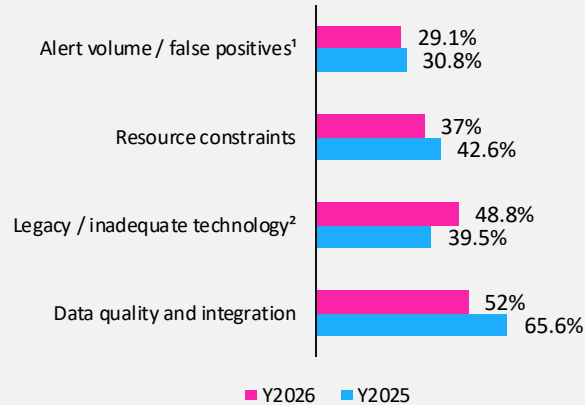
Top barriers to operational efficiency in compliance



These constraints affect more than efficiency. Fragmented data and legacy technology can also limit the ability to build a complete view of risk, prioritize activity effectively, and adapt controls as threats evolve.

Structural barriers persist despite signs of progress

Top barriers to operational efficiency in compliance, 2025-26 vs. 2026-27



¹ 2025–26 response option: “Alert fatigue”; 2026–27: “Alert volume and false positives.”

² 2025–26 response option: “Outdated or inadequate tech solutions”; 2026–27: “Legacy systems and infrastructure.” Response categories have been aligned for directional comparison.

Notably, alert volume and false positives rank below data, technology, automation, and resource constraints. This raises an important question: are high alert volumes the problem itself, or a symptom of weaknesses further upstream?

4.2 Alert management: The productivity challenge

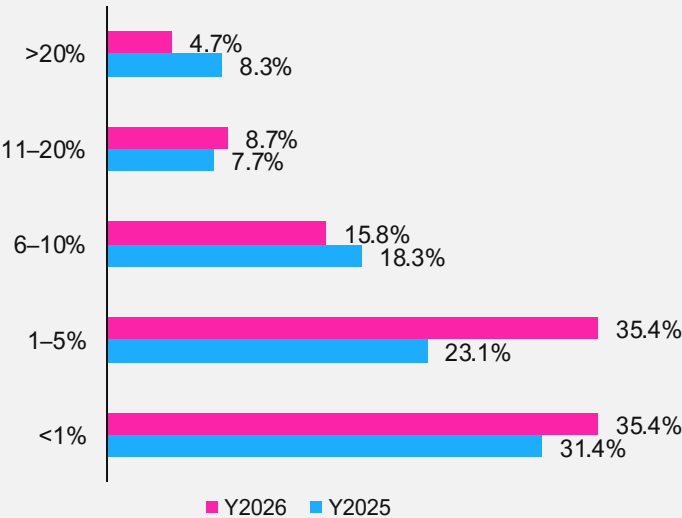
Alert management reveals the distinction between throughput and productivity. Investigations are getting faster, but low escalation yields and persistent false positives suggest that greater processing speed has not fundamentally changed the quality of the workload.

High alert volumes, limited investigative yield

Seven in ten respondents (70.8%) report that 5% or fewer alerts result in escalation or SAR/STR filing, including 35.4% where fewer than 1% do so. Only 13.4% report conversion rates above 10%.

The concentration at the lowest end of the range points to substantial alert-review activity producing relatively few escalations or filings. Low conversion does not, by itself, indicate ineffective detection – thresholds, risk appetite, and alert populations differ across institutions. But at scale, it raises an important question about the quality and prioritization of activity entering the investigative funnel.

Alert escalation and SAR/STR filing rates: 2025–26 vs. 2026–27



The year-on-year comparison makes that question more pressing. The proportion reporting escalation or filing rates of 5% or less has increased from 54.4% in 2025–26 to 70.8% in 2026–27.¹

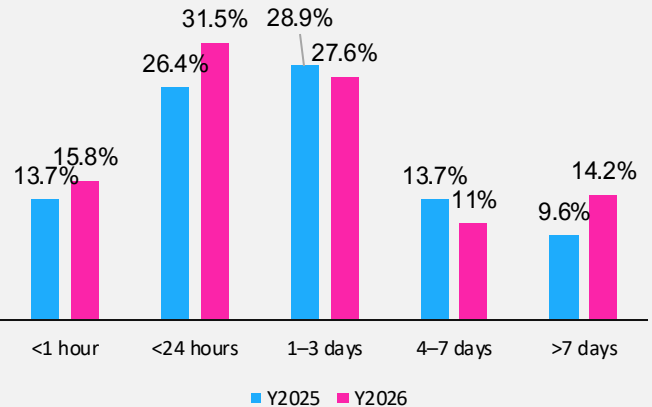
70.8% of respondents report that 5% or fewer alerts result in escalation or SAR/STR filing.

Investigations are getting faster – but not across the board

There are signs of improving processing speed. Nearly half of respondents (47.3%) now report typical investigation turnaround within 24 hours, compared with 40.1% in 2025–26. A further 27.6% typically resolve alerts within one to three days.

Yet the improvement is uneven. One in four (25.2%) take four days or longer, and the proportion reporting turnaround beyond seven days has increased from 9.6% to 14.2%.

Investigation turnaround times: 2025–26 vs. 2026–27



Note: The 2025–26 survey included a “Don’t know / Not tracked” response option (7.6%), which was not included in 2026–27. Year-on-year comparisons should therefore be interpreted directionally.

This suggests a widening range of operational performance: faster resolution at one end alongside a persistent long-duration tail at the other. The distinction matters because investigation speed alone says little about effectiveness. The objective is not simply to close alerts faster, but to resolve routine activity efficiently while preserving investigative capacity for higher-risk and more complex cases.

False positives remain a persistent drag on productivity

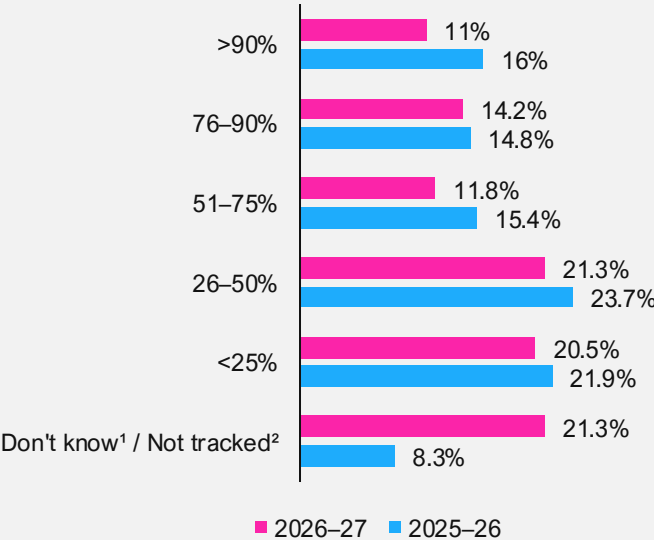
The false-positive data provides further context. More than a third of respondents (37%) report false-positive rates above 50%, including 25.2% with rates above 75%. Only 20.5% report keeping false positives below 25%.

Despite continued industry focus on alert optimization, the overall distribution has changed relatively little year over year. This suggests that reducing low-value alert activity remains a persistent challenge for many institutions.

More strikingly, 21.3% say they do not track their false-positive rate at all. Without visibility into one of the primary drivers of investigative workload, institutions may struggle to determine whether detection tuning, automation, or process changes are actually improving performance.

False-positive rates remain elevated

Reported false-positive rates:
2025–26 vs. 2026–27



Taken together, the findings reveal a more nuanced performance gap. Institutions appear to be getting faster at processing alerts, but many continue to operate with low escalation yields, high false-positive rates, or limited visibility into alert quality.

¹ 2025–26 response option.

² 2026–27 response option. Categories shown together for contextual comparison but are not directly equivalent.

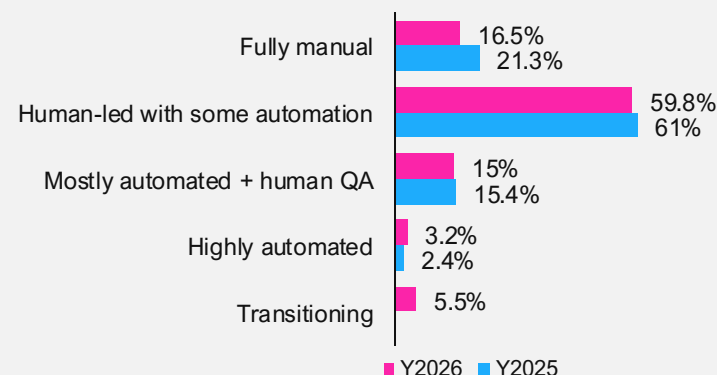


4.3 Alert review remains predominantly human-led

Despite growing investment and attention around AI, automation-led alert review has barely advanced year over year. Mostly or highly automated models account for 18.2% of respondents, compared with 17.8% across the equivalent categories in 2025–26.

Fully manual review has declined from 21.3% to 16.5%, suggesting some movement away from the most labor-intensive model. But that shift has not yet translated into materially greater adoption of automation-led review. Only 15% are mostly automated with human oversight, virtually unchanged year over year, while highly automated models remain rare at 3.2%.

**Alert review operating models show
limited year-on-year change**



**Manual review is declining, but
automation-led models remain
static**

76.3%
of alert reviews
remain fully manual
or predominantly
human-led with some
automation

The year-on-year picture suggests incremental modernization rather than a fundamental shift in the alert review model. While fewer institutions are fully manual, human review remains the primary mechanism across most compliance functions.

This is particularly significant when viewed alongside the alert productivity findings. Low escalation yields and persistently high false-positive rates mean that human investigators continue to absorb substantial review activity, limiting how far institutions can improve productivity through process optimization alone.

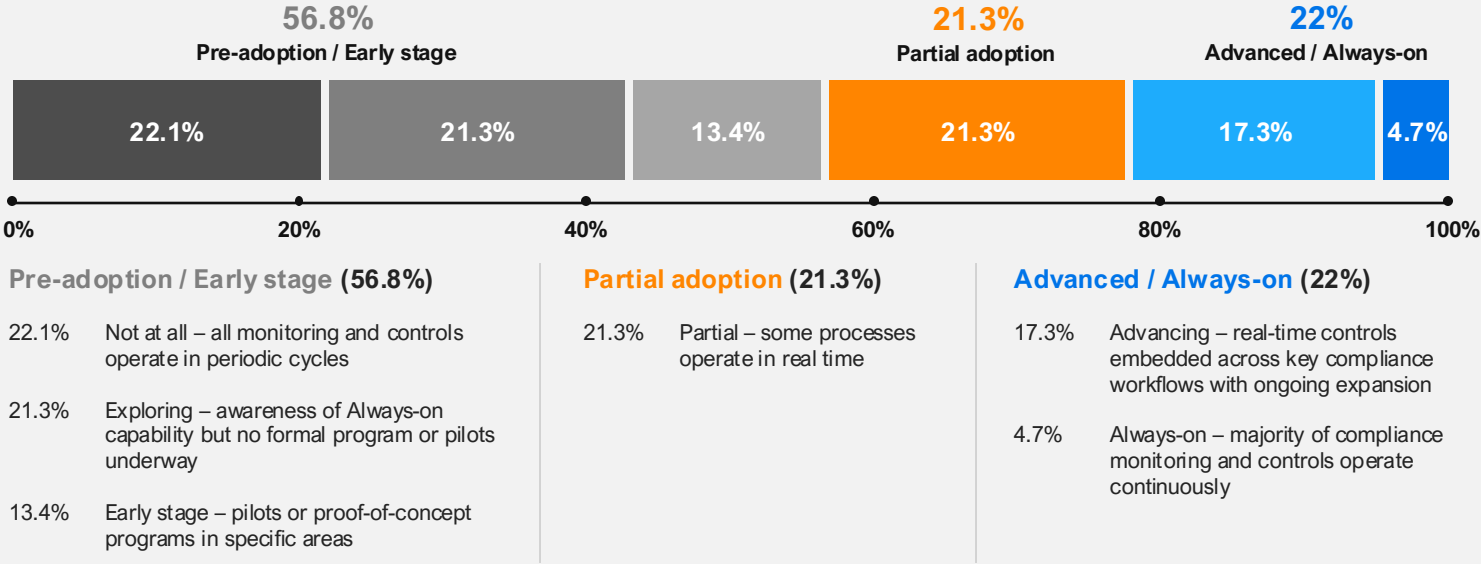
The opportunity is not maximum automation or the removal of human judgment. It is a more deliberate division of work: automating repetitive review and evidence-gathering activities while preserving human oversight for higher-risk cases, exceptions, and decisions requiring judgment and accountability. Done well, automation should improve not only capacity, but the consistency and focus of financial crime decision-making.

4.4
Always-on Compliance:
The transition has begun

The shift toward more continuous, real-time compliance is underway but remains at an early stage for much of the industry. Only 4.7% of respondents say the majority of their compliance monitoring

and controls operate continuously, while 17.3% are advancing real-time controls across key compliance workflows.

Current maturity of real-time compliance monitoring and controls



At the other end of the maturity curve, 56.8% have yet to move beyond exploration or early-stage adoption: 22.1% continue to operate entirely through periodic review cycles, 21.3% are exploring always-on capabilities without a formal program or pilots, and 13.4% are at proof-of-concept or pilot stage.

Always-on Compliance adoption remains early and uneven

Closing the effectiveness gap

The findings expose a gap between operational improvement and operational transformation. Institutions are getting faster at processing financial crime alerts, but low investigative yield, persistent false positives, limited automation, and immature continuous controls show that the underlying productivity model has changed far less.

Closing that gap requires a different objective: not simply processing the existing workload more efficiently, but improving the quality, prioritization, and risk relevance of the workload itself.

The findings expose a gap between operational improvement and operational transformation. While there are signs of progress, persistent constraints in data, technology, alert quality, automation, and continuous controls show that the underlying operations has changed far less.

Closing this gap requires a different objective: not simply processing existing compliance activity more efficiently, but improving its quality, prioritization, and ability to deliver meaningful risk and compliance outcomes.

What should compliance leaders do now?

Measure outcomes, not just throughput.

Move beyond alert counts and closure speed. Track escalation yield, false-positive rates, investigation time, disposition, and outcomes together to understand whether controls are directing capacity toward meaningful risk and effective outcomes.

Reduce low-value work at source.

Do not treat investigation efficiency as solely an investigator problem. Address the data quality, fragmented technology, detection logic, and limited contextual intelligence that create unnecessary activity upstream.

Automate work, not accountability.

Use automation to absorb repetitive data gathering, enrichment, triage, and case preparation while retaining appropriate human judgment and accountability for higher-risk and consequential decisions.

Close the measurement gaps.

Establish consistent baselines for alert quality, investigation performance, and outcomes so that changes to detection, automation, and technology can be evaluated against measurable results and improved effectiveness over time.

Build a deliberate path to continuous compliance.

Move beyond periodic processing and reactive practices by progressively connecting changing risk signals to continuous monitoring, assessment, and control responses. Prioritize areas where real-time insight improves risk detection and intervention, then expands as data, technology, automation, and governance mature.

Key takeaway

The next productivity gains in financial crime compliance will come less from processing the existing workload faster and more from changing the workload itself.

Closing the effectiveness gap means reducing low-value activity before it consumes investigative capacity, improving risk-based prioritization, and applying automation where it can augment human expertise. The result is not simply a more efficient compliance function, but one that is more effective, scalable, and resilient as risks and regulatory expectations evolve.

AI moves from experimentation to enterprise capability

AI’s narrative in financial crime compliance is changing. A year ago, the dominant question was whether to adopt. Today, the question is how to scale AI safely, effectively and with appropriate oversight.

This year’s findings show meaningful progress from experimentation toward practical application, but enterprise capability remains much less mature. AI is gaining ground across transaction monitoring, sanctions screening, KYC/CDD and fraud detection, yet most organizations remain at or below the pilot stage and automation remains limited across the wider financial crime operating model.

The next challenge is scale. Moving AI from individual use cases into production requires more than technology: it depends on integrated data, operational governance, explainability and clear human

accountability. The findings reveal an important distinction between organizations that are using AI and those building the foundations to operationalize it at enterprise scale.

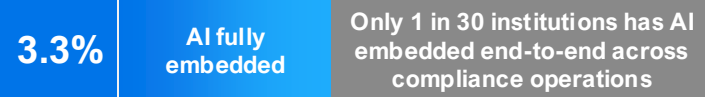
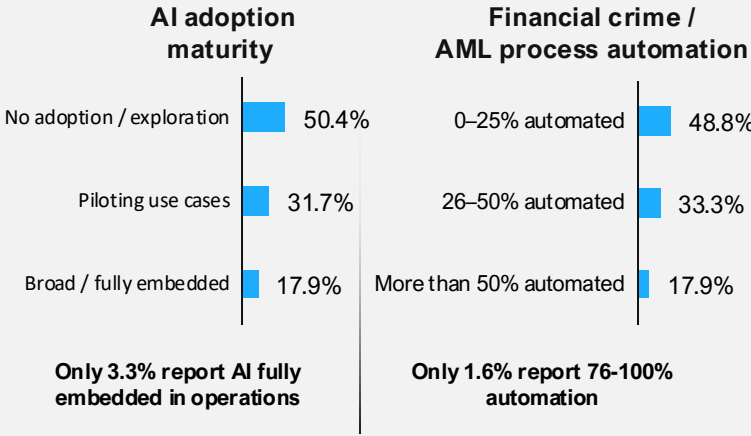
5.1 From experimentation to enterprise capability

The overall picture is one of early-stage momentum, not yet enterprise scale. More than four in five organizations (82.1%) remain at or below the pilot stage of AI adoption: 20.3% report no adoption, 30.1% are in early exploration and 31.7% are piloting use cases. Only 17.9% report broad implementation or fully embedded AI, and just 3.3% say AI is fully embedded and integrated into operations.

Much of this has to do with the quick pace of AI advancement, budgets, fitting-in with larger internal AI programs, and understanding the direction of new and complimentary AI use cases in FinCrime.

The same maturity pattern is visible in automation. Some 82.1% have automated no more than half of their financial crime and AML processes, including 48.8% with automation across just 0–25%. Only 17.9% have automated more than half.

AI maturity and process automation, 2026–27

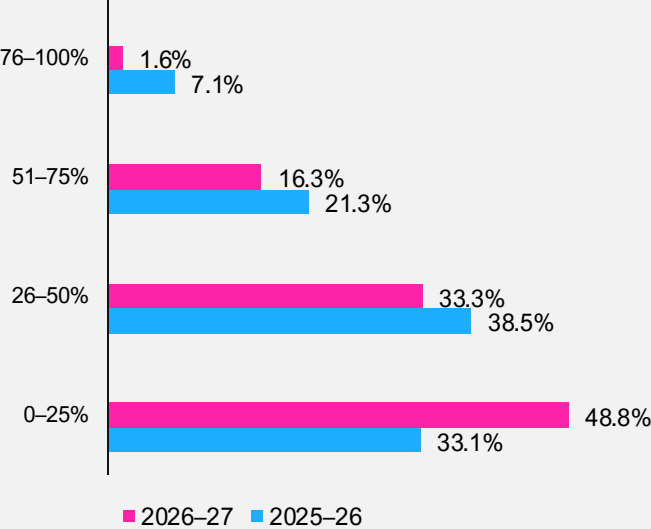


82.1% at or below the AI pilot stage.
82.1% have automated 50% or less of their financial crime processes.

Taken together, the findings expose the gap between adopting AI and building enterprise capability. Organizations are increasingly experimenting with AI, but most have yet to translate that activity into automation at scale.

The year-on-year automation picture reinforces that point. In 2025–26, 71.6% reported automation across no more than half of their AML program; this year, that figure stands at 82.1% across financial crime/AML processes. The 0–25% cohort has increased from 33.1% to 48.8%.

Process automation: 2025–26 vs. 2026–27



Note: Year-on-year results reflect different respondent samples. The 2025–26 question referred to the “AML program”; the 2026–27 question refers to “financial crime / AML processes.” Comparisons should therefore be interpreted directionally.

The next phase of AI maturity will therefore be defined not by how many organizations can demonstrate

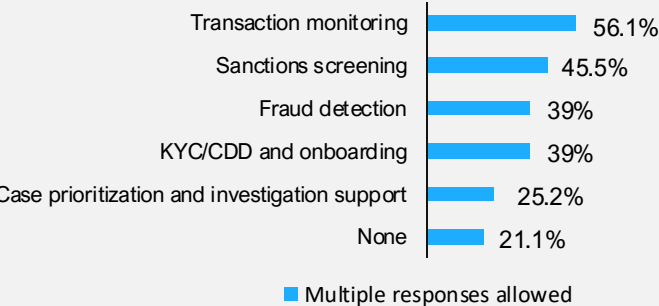
successful use cases, but by how effectively they can move them into production, integrate them across workflows and translate AI investment into sustainable operational change.

Financial crime compliance has entered the AI experimentation era, but not yet the AI operating era.

5.2
AI is gaining ground – but unevenly

AI adoption is nevertheless spreading across the financial crime lifecycle. Transaction monitoring is the most widely reported use case at 56.1%, followed by sanctions screening at 45.5%. Fraud detection and KYC/CDD and onboarding both stand at 39%, while case prioritization and investigation support remains less widely adopted at 25.2%.

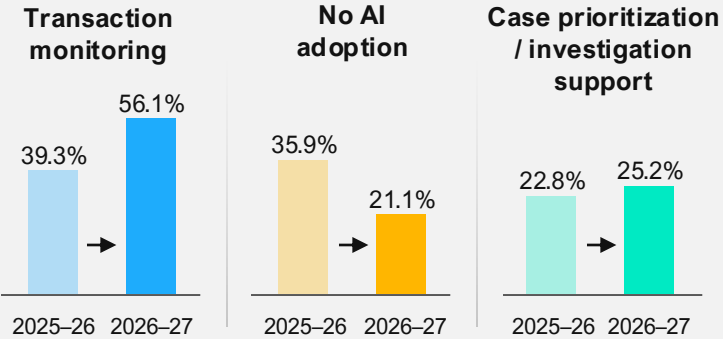
AI use cases currently deployed in financial crime compliance



The direction of travel is clearer where comparison with last year is possible. Transaction monitoring has risen from 39.3% to 56.1%, while the proportion reporting no AI adoption has fallen from 35.9% to 21.1%. Case prioritization and investigation support has moved more modestly, from 22.8% to 25.2%.

AI is gaining ground

Change in % of respondents applying or not applying AI in key use cases



Note: Multiple responses allowed. 2025–26 question: “Which areas has your organisation implemented or piloted AI/ML solutions, if any?” 2026–27 question: “Which use cases are you currently applying AI to in financial crime compliance?”

AI adoption is broadening, but unevenly. Established detection and screening use cases are moving ahead faster than investigation support, suggesting that breadth of adoption is developing faster than end-to-end transformation.

5.3

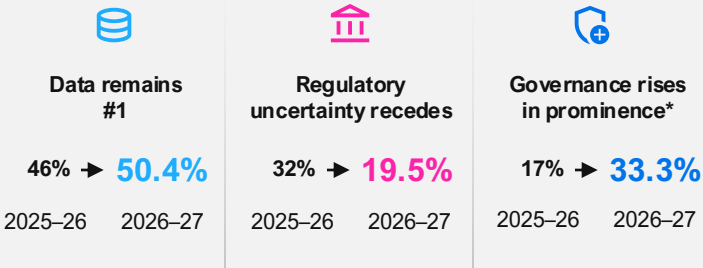
Scaling AI exposes the foundations beneath it

As organizations move from experimentation toward production, the barriers to adoption are changing. Data quality, availability and integration remains the leading constraint, cited by 50.4% of respondents. Technology and infrastructure limitations follow at 39.8%, while model governance, explainability and auditability now rank third at 33.3%.

Skills and talent scarcity, and difficulty justifying ROI, are each cited by 30.9%, while vendor maturity, organizational culture and regulatory uncertainty rank lower.

The year-on-year picture is particularly revealing. Data remains the dominant issue, rising directionally from 46% to 50.4%. Regulatory uncertainty, by contrast, has fallen from 32% to 19.5%. Governance has moved in the opposite direction: model governance was cited by 17% last year, compared with 33.3% citing the broader category of governance, explainability and auditability this year.

The barriers are shifting



*Question wording evolved to include explainability and auditability; directional comparison only.

The changing barrier profile points to a more mature set of concerns. Organizations are still wrestling with the infrastructure required to deploy AI. Moving from pilots into production requires connected and reliable data, technology capable of supporting AI across workflows, and governance that provides appropriate transparency, control and accountability.

Data is the common constraint. In Chapter 4, 52% of respondents identified data quality and integration as a barrier to operational efficiency; here, 50.4% identify data quality, availability and integration as a barrier to AI-driven detection. The implication is significant: the same data limitations affecting today's financial crime operations risk constraining the next generation of AI-enabled capabilities.

5.4

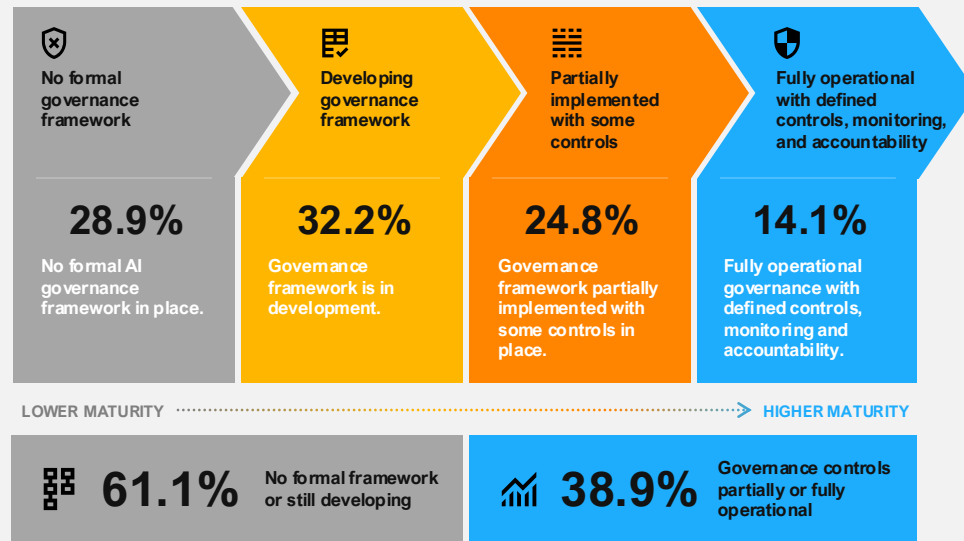
Building trusted AI – governance maturity

Governance is emerging as a critical part of the AI scaling challenge. While a third of respondents (33.3%) identify model governance, explainability and auditability requirements as a barrier to AI-driven proactive detection, the underlying governance capability remains immature.

More than six in ten organizations (61.1%) either have no formal AI governance framework or are still developing one. A further 24.8% have partially implemented governance with some controls in place. Only 14.1% report a fully operational approach with defined controls, monitoring and accountability. Without mature governance, AI risks scaling existing control weaknesses rather than transforming them.



AI governance maturity continuum



The findings point to a gap between establishing governance principles and operationalizing them. Enterprise AI requires more than policies or approval structures: governance needs to extend into ongoing model monitoring, validation, accountability and control throughout the AI lifecycle. As AI moves into production, the challenge shifts from defining governance principles to embedding them in day-to-day operations.

5.5

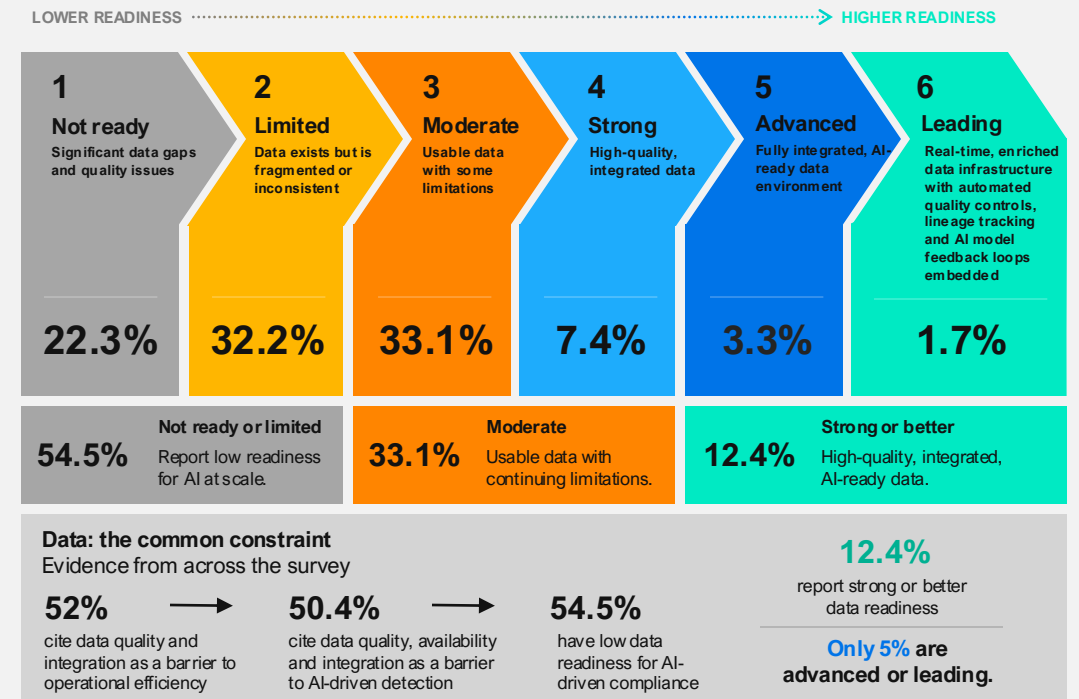
AI ambition is running ahead of data readiness

The data foundations required to scale AI remain underdeveloped. More than

half of respondents (54.5%) describe their organization's data readiness for AI-driven compliance as either not ready or limited, including 32.2% whose data exists but remains fragmented or inconsistent. A further 33.1% report moderate readiness, with usable data but continuing limitations.

Only 12.4% assess their data readiness as strong or better. At the upper end of the maturity curve, just 5% report an advanced or leading environment, characterized by fully integrated, AI-ready data or real-time enriched infrastructure with automated quality controls, lineage tracking and AI model feedback loops.

Data readiness continuum



The findings reinforce the barrier identified earlier in the chapter. Half of respondents (50.4%) cite data quality, availability and integration as an obstacle to AI-driven proactive detection. The issue also extends beyond AI: 52% identified data quality and integration as a barrier to operational efficiency in Chapter 4.

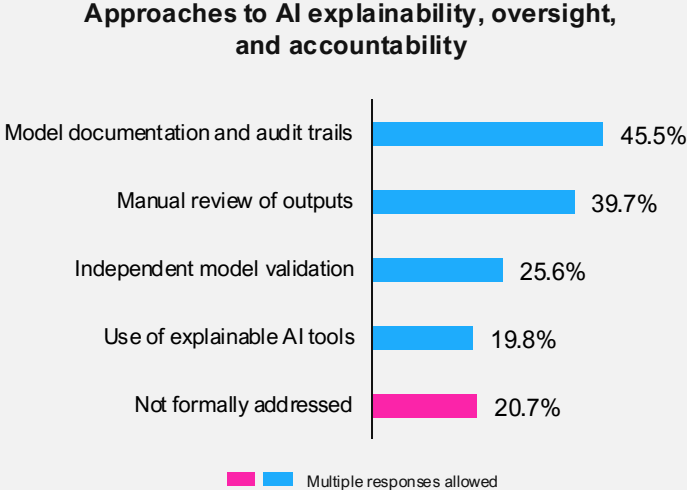
Last year's findings provide further context. Data fragmentation across systems was the most frequently cited data challenge at 48.9%, followed by incomplete or outdated data at 45.4%; only 11% of respondents said they were very confident that their data was clean, traceable and governed.

The consistency of these findings is significant. Data is not simply an AI implementation issue; it is a common constraint across operational efficiency, model effectiveness and enterprise transformation.

5.6 Explainability is becoming operational – but remains human-led

As AI adoption expands, organizations are putting greater emphasis on the controls required to make its use transparent and accountable. Model documentation and audit trails are the most widely used mechanism, cited by 45.5% of respondents,

followed by manual review of AI outputs at 39.7%. Independent model validation is used by 25.6%.



The year-on-year picture suggests that formal attention to explainability is increasing, but technical adoption is not advancing at the same pace. The proportion saying explainability is not formally addressed has fallen from 33.1% to 20.7%, while documentation and audit trails have increased directionally from 41.4% to 45.5%. Yet use of dedicated explainable AI tools remains virtually unchanged, at 19.8% compared with 19.3% last year.

Explainability is evolving – but explainable AI adoption is not

Year-over-year comparison of explainability practices

	2025–26 (% of respondents)	2026–27 (% of respondents)
 Not formally addressed	33.1%	20.7% 
 Documentation / audit trails*	41.4%	45.5% 
 Explainable AI tools	19.3%	19.8% 



Formal attention to explainability is increasing, but technical XAI adoption remains largely unchanged.

*2025 measured documenting model logic and decision paths; 2026–27 measures model documentation and audit trails. Directional comparison only.

This suggests that organizations are strengthening explainability primarily through documentation, governance and human oversight rather than through technical explainable AI capabilities. Last year's survey reinforces this picture: human reviewers played central roles in validating alert relevance, making final case decisions and interpreting grey-area outputs. This year's reliance on manual review provides further evidence that human oversight remains an important part of AI-supported compliance.

As AI systems become more complex and autonomous, the challenge will be to preserve that human judgment while making explainability, validation, monitoring and accountability systematic and scalable.

From proving AI to operationalizing it

Financial crime compliance is approaching an important transition point in its use of AI. The question is no longer whether AI can improve detection, prioritization or decision support, but whether financial institutions can turn individual successes into repeatable, governed enterprise capabilities.

This year's findings show why that transition remains difficult. AI is spreading across individual use cases faster than it is becoming embedded across financial crime operations. At the same time, the capabilities required to scale it – integrated data, resilient technology, mature model governance and explainability – remain underdeveloped across much of the industry.

This changes the nature of the AI agenda. The next stage will not be won by accumulating more proofs of concept. Leading organizations will need to connect AI investment to operating-model redesign: identifying where AI materially improves effectiveness or

efficiency, industrializing successful applications, establishing controls across the AI lifecycle and defining where human judgment remains essential.

The objective should not be maximum automation, but better orchestration between AI, automation and human expertise – with AI providing speed, scale and intelligence while people retain appropriate oversight and accountability for consequential decisions. That is the foundation for AI that is not only more effective and efficient, but also explainable, defensible and resilient.

AI Maturity Model

	1. Exploring	2. Piloting	3. Scaling	4. Enterprise AI
AI deployment	Isolated exploration	Defined use cases	Multiple production use cases	Embedded across workflows
Automation	Predominantly manual	Selective automation	Connected automation	Orchestrated across workflows
Data	Fragmented / inconsistent	Usable and integrated	Real-time, enriched and partially governed	Unified, continuously enriched and governed
Governance	Informal	Framework developing	Controls implemented	Continuous governance and monitoring
Explainability	Manually documented	Documented, reviewed and auditable	Validated, traceable and integrated	Continuous, transparent and embedded across the AI lifecycle
Human role	Performs workflow	Reviews AI outputs	Exception handling and judgment	Human-in-command oversight

Note: The maturity model is an interpretive framework derived from the survey findings. It does not assign individual respondents to maturity stages.

Why it matters

The enterprise AI challenge is shifting from experimentation to execution. As adoption expands, value will increasingly depend on whether institutions can move successful use cases into production and integrate them into end-to-end financial crime workflows.

That makes data, governance and explainability operational requirements rather than supporting considerations. Strong data, effective governance and clear explainability are essential to scaling AI responsibly across financial crime compliance. Together, these foundations can enable institutions to scale AI with greater confidence while preserving the transparency, control and human accountability.

What leaders should do?

Industrialize what works

Move successful AI use cases beyond pilots by establishing clear production pathways, integration requirements, ownership and measures of business and compliance value. Prioritize applications that can demonstrate improvements in effectiveness or efficiency rather than expanding the number of experiments.

Treat data readiness as a strategic compliance priority

Address fragmentation, quality, lineage and accessibility as part of the financial crime transformation agenda. AI-ready data architecture should support model performance and traceability, explainability and ongoing control.

Operationalize AI governance

Move beyond frameworks and policies towards embedded controls throughout the AI lifecycle – including validation, monitoring, documentation, escalation and defined accountability. Governance should enable responsible scaling rather than operate as a downstream approval process.

Design human oversight into the operating model

Define where human judgment adds the greatest value and where automation can safely absorb repetitive work. As AI capabilities become more autonomous, establish clear decision rights, intervention points and accountability so that human oversight evolves with the technology rather than becoming an operational bottleneck.

Key insights

AI adoption is real, but enterprise maturity remains limited

More than eight in ten organizations remain at or below the pilot stage, while only 3.3% report fully

embedded AI.

AI is spreading faster than automation is scaling

Transaction monitoring adoption has risen directionally to 56.1%, yet 82.1% still have half or less of their financial crime processes automated.

Data remains the common constraint

Data is the leading barrier to AI-driven detection, while 54.5% report low data readiness. The same issue also constrains operational efficiency.

Trusted AI requires operational governance

61.1% have no formal governance framework or are still developing one; only 14.1% have reached fully operational governance.

Explainability remains predominantly process- and human-led

Documentation and manual review lead current approaches, while dedicated explainable AI adoption remains at 19.8%.

Enterprise capability is the next frontier

AI use is expanding, but enterprise capability is not defined by adoption alone. The next maturity threshold is the ability to scale AI through automation, data, governance, explainability and human accountability.

The future financial crime operating model

Financial crime compliance is moving toward greater use of AI, automation and real-time capabilities. The survey points to a growing role for AI, connected data and risk intelligence in how financial crime is detected, investigated and managed.

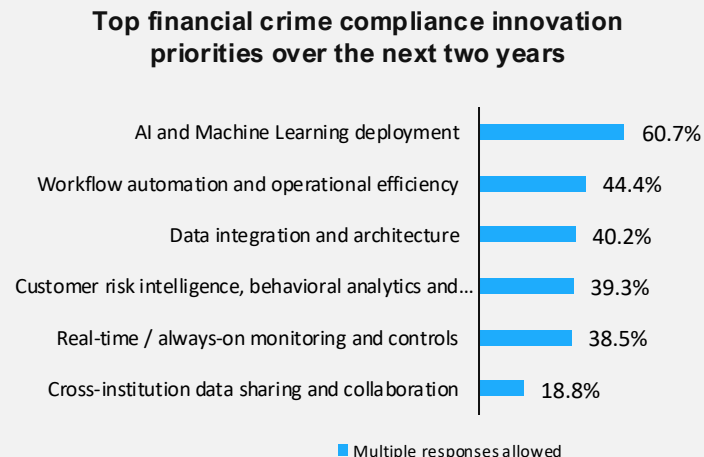
Yet the findings do not point to a fully autonomous future. Instead, they suggest a changing division of work between people and technology, with AI taking on a greater share of execution while human expertise remains central to judgment, oversight and accountability.

The transition will require more than AI deployment alone. Institutions are prioritizing workflow automation, data integration, dynamic customer risk intelligence and always-on monitoring alongside AI and machine learning. At the same time, budget constraints, data limitations and legacy technology continue to restrict the pace of innovation.

The financial crime operating model of the future will therefore be defined not simply by how much technology it adopts, but by how effectively it combines AI, intelligence, automation and human judgment to deliver stronger compliance outcomes.

6.1 AI leads the innovation agenda

AI and machine learning have moved to the top of the financial crime innovation agenda. More than six in ten respondents (60.7%) identify AI and machine learning deployment as a priority for the next two years, ahead of workflow automation and operational efficiency (44.4%), data integration and architecture (40.2%), and customer risk intelligence, behavioral analytics and dynamic risk scoring (39.3%).



The wider priorities also show that AI is only one part of the innovation agenda. Workflow automation, integrated data, dynamic risk intelligence and real-time monitoring are complementary capabilities: together, they provide important foundations for deploying AI effectively across financial crime workflows and supporting more adaptive, intelligence-led approaches to risk.

AI has moved further up the strategic agenda. In 2025–26, 45% of respondents planned to augment their existing technology stack with newer innovations such as AI agents. This year, 60.7% identify AI and machine learning deployment among their top innovation priorities. While the questions are not directly equivalent, the comparison is consistent with AI becoming a more prominent part of the financial crime innovation agenda.

The challenge now is to translate that ambition into operational capability. As Chapter 5 showed, AI maturity, data readiness and governance remain uneven. Realizing the value of AI investment will depend on institutions' ability to strengthen these foundations and move successful use cases into production at scale.

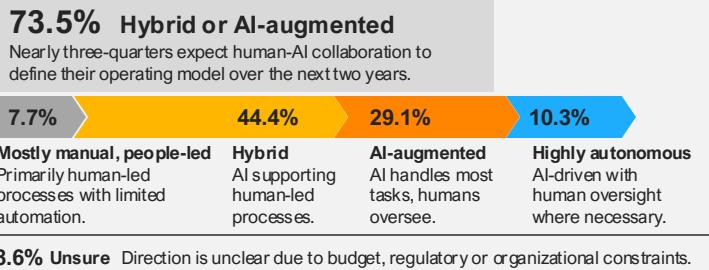
6.2

The future is augmented, not autonomous

The expected operating model of the future is overwhelmingly one of human-AI collaboration. Nearly three-quarters of respondents (73.5%) expect their financial crime compliance function to operate through either a hybrid model, with AI supporting human-led processes (44.4%), or an AI-augmented model, where AI handles most tasks and humans provide oversight (29.1%).

Only 10.3% expect to move to a highly autonomous model over the next two years, where operations are largely AI-driven with human oversight where necessary. A further 7.7% expect their operating model to remain mostly manual and people-led, while 8.6% remain unsure of the direction because of budget, regulatory or organizational constraints.

Expected evolution of the financial crime compliance operating model over the next two years.



The findings reveal an important distinction between technology ambition and operating-model expectations. While AI and machine learning lead the innovation agenda, most institutions do not expect that investment to result in highly autonomous operations within the next two years. Instead, the dominant expectation is augmentation: AI taking on more work with human judgement and oversight remaining central.

6.3

Agentic AI moves into operational execution

Respondents see the greatest potential in alert triage and prioritization (57.3%), KYC/CDD and perpetual due diligence (50.4%), and investigations and case management (41%). By comparison, only 24.8% identify cross-functional orchestration across fraud, AML and sanctions as a leading opportunity.



These priorities point toward a pragmatic path for Agentic AI adoption. Rather than beginning with highly autonomous decision-making, institutions see greater potential in using AI agents to gather and assess information, prioritize work, coordinate steps and support the progression of cases through complex compliance workflows. More cross-functional applications currently rank lower: 24.8% identify orchestration across fraud, AML and sanctions as a leading opportunity, while model monitoring and governance (15.4%) and regulatory reporting (11.1%) sit further down the list.

The ranking also suggests that institutions see the strongest near-term case for Agentic AI where work is information-intensive, repetitive and dependent on coordinating multiple steps. Governance and regulatory reporting rank lower, indicating greater caution around use cases where control, validation and accountability requirements are particularly significant. As confidence, governance and explainability mature, this could create a pathway for Agentic AI to move beyond task automation and support increasingly complex analysis and decision-making across financial crime processes.

6.4

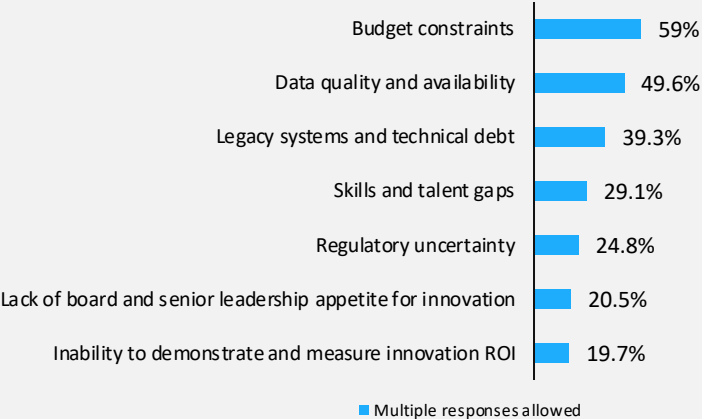
The innovation gap is becoming an execution gap

The ambition to innovate is clear, but the ability to

execute remains constrained. Budget is the leading constraint, cited by 59% of respondents, followed by data quality and availability (49.6%) and legacy systems and technical debt (39.3%).

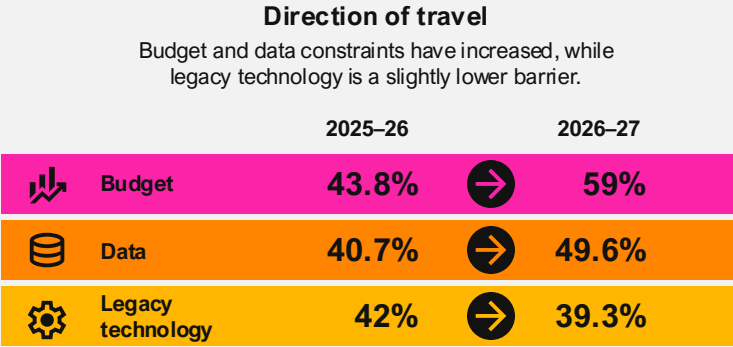
Skills and talent gaps remain a challenge for 29.1% of respondents and regulatory uncertainty for 24.8%, but both rank below the financial, data and technology constraints affecting organizations' ability to modernize.

Top barriers to innovation in financial crime compliance



The pattern is also visible year over year. In 2025–26, budget, legacy technology and data were already among the leading limitations to building a future-ready compliance technology stack. This year, they remain the three leading barriers to innovation, with budget pressure particularly pronounced. The comparison is directional, but it suggests that

innovation ambitions continue to run ahead of some of the foundations required to deliver them.



Directional comparison only; question wording changed between survey years.

Taken together, the findings suggest that innovation will depend not only on investment in new capabilities, but on institutions' ability to address the budget, data and technology constraints that continue to limit execution at scale.

DATA: Different challenges, same constraint

- 52% barrier to operational efficiency
- 50.4% barrier to AI-driven detection
- 49.6% barrier to innovation

Data remains a persistent constraint across financial crime operations, AI adoption and innovation.

6.5 What will define the next-generation financial crime function

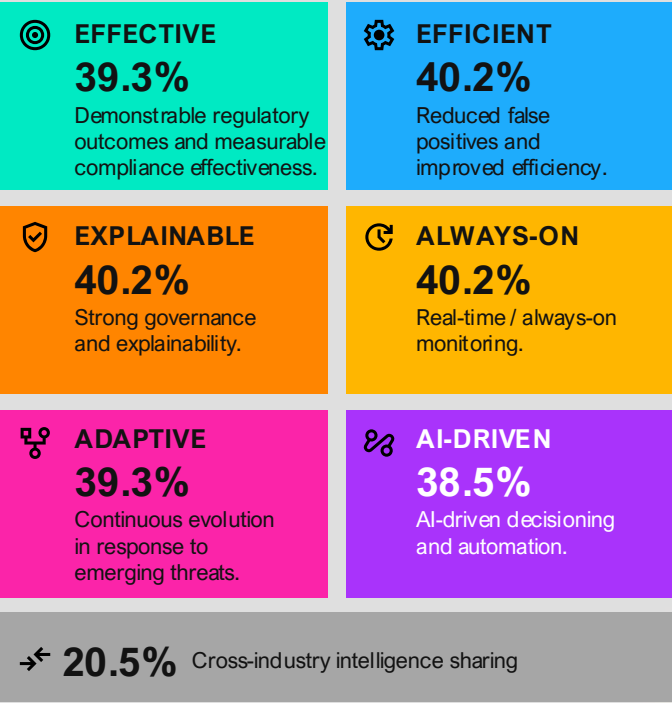
The future function is not being defined by automation alone. Respondents place remarkably similar weight on efficiency, effectiveness, governance and explainability, adaptability, always-on monitoring and AI-driven decisioning.

Real-time / always-on monitoring, reduced false positives and improved efficiency, and strong governance and explainability each rank highest at 40.2%. Close behind are demonstrable regulatory outcomes and measurable compliance effectiveness (39.3%) and an adaptive operating model that continuously evolves in response to emerging threats (39.3%). AI-driven decisioning and automation follows at 38.5%.

No single answer dominates. Just 1.7 percentage points separate the six leading characteristics of high performance, pointing to a future financial crime function that is multidimensional rather than defined by any single capability.

The next-generation financial crime function

Six capabilities shaping the future financial crime function



KEY FINDING:
High performance will be multidimensional.

No single capability dominates the definition of the future financial crime function. Effectiveness, efficiency, explainability, always-on monitoring, adaptability and AI-driven decisioning all rank within 1.7 percentage points of one another.

What leaders should do?

Treat operational automation as a starting point, not the destination.
Prioritize use cases that demonstrate measurable value. Alert triage, KYC/CDD and investigations offer clear opportunities for Agentic AI. Use these workflows to demonstrate value and build experience before extending AI into more complex financial crime processes.

Build the data and governance foundation for scale.
Data remains a recurring constraint across operational efficiency, AI adoption and innovation, while AI governance maturity remains limited. Data architecture, explainability, monitoring and accountability need to develop alongside AI deployment, not be addressed only after solutions move into production.

Build the business case around outcomes.
With budget cited by 59% as the leading barrier to innovation, investment cases will need to demonstrate more than technology deployment. Link investment to measurable improvements in false-positive reduction, investigation performance, compliance effectiveness and regulatory outcomes.

Redesign human roles and accountability as automation expands.
As AI takes on more execution, institutions will need clarity over where human judgment, oversight and accountability remain essential. The objective should be to redirect expertise toward complex decisions, emerging risks and governance while maintaining clear accountability across increasingly automated workflows.

These findings bring together the three dimensions that have emerged throughout this report: effectiveness, efficiency and explainability. Increasingly, they will need to operate within a financial crime function that is also adaptive and always-on, able to respond continuously as customer behavior, threats, data and regulatory expectations evolve.

The next-generation financial crime function will therefore be defined not by a single technology or operating model, but by its ability to combine these capabilities: using AI and automation to execute at greater speed and scale, risk intelligence to adapt to changing risk, and strong governance and human oversight to maintain trust and accountability.

CONCLUSION

From AI ambition to operating reality

The FinCrime Frontier 2026–27 findings point to an industry at an important transition. Financial institutions are navigating evolving regulatory expectations, persistent cost and resource pressures, changing financial crime threats and rapid advances in AI. Across the survey, the direction of travel is clear: institutions recognize the need to modernize. The harder challenge is translating that ambition into measurable improvements in financial crime outcomes.

That challenge runs through the findings. Regulatory change is influencing transformation and operating-model decisions, while technology and systems remain the largest cost driver. AI and automation have become the leading investment priority yet approaches to measuring return on compliance investment remain relatively immature. Operationally, institutions are making progress in processing work, but there is less evidence of fundamental change in the quality and composition of that work to drive improved effectiveness. And while AI is gaining ground across transaction monitoring, sanctions screening and fraud detection, most institutions remain at or below the pilot stage of AI maturity.

The foundations for the next stage of transformation are also still developing. Data remains the most significant barrier to AI-driven proactive detection, governance maturity is uneven, and only

a small minority describe their data readiness as strong, advanced or leading. Always-on monitoring, meanwhile, remains an aspiration for much of the market rather than an established capability.

For financial crime leaders, the implication is clear: the next phase of transformation cannot be measured by technology adoption alone. The more important question is whether investment improves the institution's ability to identify, understand and respond to financial crime risk – while maintaining the governance, transparency and accountability required to demonstrate that controls remain effective.

Three priorities emerge from the research.

Effectiveness must remain the primary measure of progress.

Faster processing and lower alert volumes can improve performance, but they do not by themselves demonstrate that a financial crime program is working. Institutions need stronger evidence that controls identify relevant risk, improve detection quality and adapt as threats evolve. That means measuring outcomes alongside traditional measures of activity and throughput.

Efficiency must come from redesign, not automation in isolation. Automating existing processes can reduce manual effort and accelerate individual tasks. Greater value can come from connecting data, detection, investigation and decision-making across financial crime workflows. The objective is to reduce unnecessary work, direct human expertise toward higher-value decisions and respond to risk more effectively.

Explainability must advance with AI adoption. As AI plays a greater role in detection, prioritization and investigation, institutions need to be able to understand, govern and defend how those capabilities are used. Transparency, validation, auditability and appropriate human oversight therefore need to develop alongside AI itself.

Together, these priorities point toward a financial crime operating model that is more connected, adaptive and intelligence-led: one that can use risk intelligence more effectively across processes, apply automation where it adds measurable value and combine AI with human judgment and accountability.

The transition will be incremental. Early AI and automation initiatives demonstrate value and build confidence, while creating the case for deeper investment in data, architecture, governance and connected workflows. The critical shift is from isolated use cases to sustainable enterprise capability, with each investment contributing to stronger financial crime outcomes rather than adding another layer of technology or complexity.

For financial crime compliance leaders, this makes the leadership challenge broader than choosing where to deploy AI. It is about establishing the data, governance, skills, technology and operating disciplines that allow innovation to scale without weakening control, accountability or regulatory confidence.

By 2030, the distinction between leaders and laggards may therefore be less about who adopted AI first than who successfully translated investment and innovation into measurable and defensible financial crime capability. High-performing institutions will be those that can demonstrate that their controls are effective, their operations efficient, their use of AI explainable, and their operating models resilient enough to adapt as risks and regulatory expectations change.

The next frontier in financial crime compliance is translating innovation into measurable outcomes - greater effectiveness, efficiency and explainability at scale.

Acknowledgment of contributors

The FinCrime Frontier 2026–27 report would not have been possible without the participation of the financial crime and compliance community. We extend our sincere thanks to all survey respondents for sharing their time, experience and perspectives. Their contributions provide a valuable, data-driven view of how financial institutions are responding to evolving financial crime risks, regulatory expectations, operational pressures and the growing role of AI.

We also thank the SymphonyAI Financial Services and AML Intelligence teams for their collaboration in the research, analysis and development of this report. Their collective industry expertise and perspectives helped bring context to the findings and explore what they mean for the future of financial crime compliance.

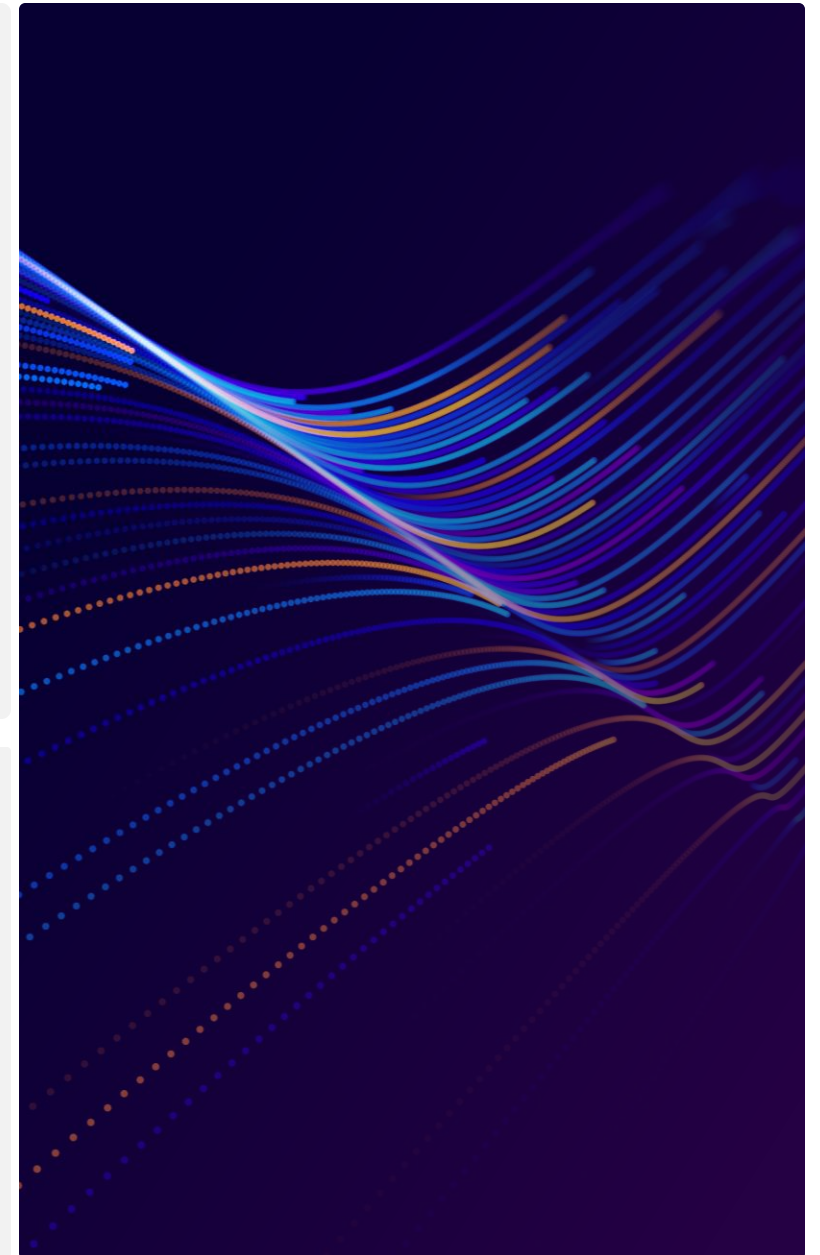
Finally, we are grateful to the wider financial crime community whose ongoing dialogue, challenge and experience continue to advance thinking on how financial institutions can build more effective, efficient, explainable and resilient financial crime operations.

SymphonyAI Financial Services

John Edison, President, Financial Services
Charmian Simmons, Principal Strategic Advisor,
FinCrime Compliance
Priya Aggarwal, Head of Global Marketing
Lala Huseynli, Financial Services Marketing & Growth
Lead, EMEA
Henry Fosdike, Global Content Manager
Bianca Malisan, Head of Creative Services

AML Intelligence

Stephen Rae, Co-Founder and Chair
James Treacy, Co-Founder and Managing Director
Mortimer O'Sullivan, Chief Technology Officer
Paul O'Donoghue, Senior Correspondent
Alisha Houlihan, Marketing Manager
Chloe Regan, Digital Marketing Executive



About SymphonyAI

SymphonyAI, 2024 Microsoft Partner of the Year for Business Transformation – AI Innovation, is building the leading enterprise AI SaaS company for digital transformation across the most critical and resilient growth verticals, including retail, consumer packaged goods, finance, manufacturing, media, and IT/enterprise service management. SymphonyAI verticals have many leading enterprises as clients. Since its founding in 2017, SymphonyAI has grown rapidly to 3,000 talented leaders, data scientists, and other professionals. SymphonyAI is a SAI Group company, backed by a \$1 billion commitment from Dr. Romesh Wadhvani, a successful entrepreneur and philanthropist.

SymphonyAI provides AI-focused SaaS solutions developed from the ground up for fighting financial crime. An end-to-end offering compiled from more than 25 years of knowledge in tackling money laundering and fraud, our award-winning product ecosystem comprises an innovative and modern approach to financial crime investigation using world-leading agentic, predictive, and gen AI. From KYC/CDD and transaction monitoring through to payments fraud, entity resolution, and sanctions, PEP, and adverse media screening, SymphonyAI is a trusted name in finance technology with more than a third of the world's top 100 banks enjoying the power, efficiency, effectiveness and productivity that our solutions provide.



www.symphonyai.com



About AML Intelligence

AML Intelligence delivers trusted Business Intelligence on Anti-Money Laundering (AML) and Financial Crime for executive leaders worldwide.

We are dedicated to delivering high-quality journalism, analysis, and data-driven insights on money laundering, terrorist financing, and broader financial crime issues.

Our mission is to empower the AML community through authoritative content, professional events and valuable networking opportunities that foster continuous learning and collaboration in the fight against financial crime.

With a foundation built on integrity, accuracy, and credibility, AML Intelligence is your trusted source for understanding new regulations, legislation, and industry thought leadership.

For AML leaders and executives, the smartest way to stay ahead is to attend our events and subscribe to our newsletters, your gateway to expert insights and community connection.



www.amlintelligence.com



Research disclaimer

This report is based on research conducted by SymphonyAI and AML Intelligence and reflects the views and experiences reported by survey respondents. The findings are provided for general informational purposes and should not be interpreted as legal, regulatory, financial, or professional advice. Survey results represent the respondent sample and should not be considered statistically representative of the financial services industry as a whole.

While reasonable efforts have been made to ensure the accuracy and reliability of the information presented, SymphonyAI and AML Intelligence make no representation or warranty as to its completeness or accuracy and accept no liability for decisions made or actions taken based on the information contained in this report.

© 2026 SymphonyAI and AML Intelligence. All rights reserved.

This publication may be quoted or referenced for non-commercial purposes with appropriate attribution to *FinCrime Frontier 2026–27*, *SymphonyAI* and *AML Intelligence*. Reproduction or distribution of substantial portions of the publication requires prior written permission.