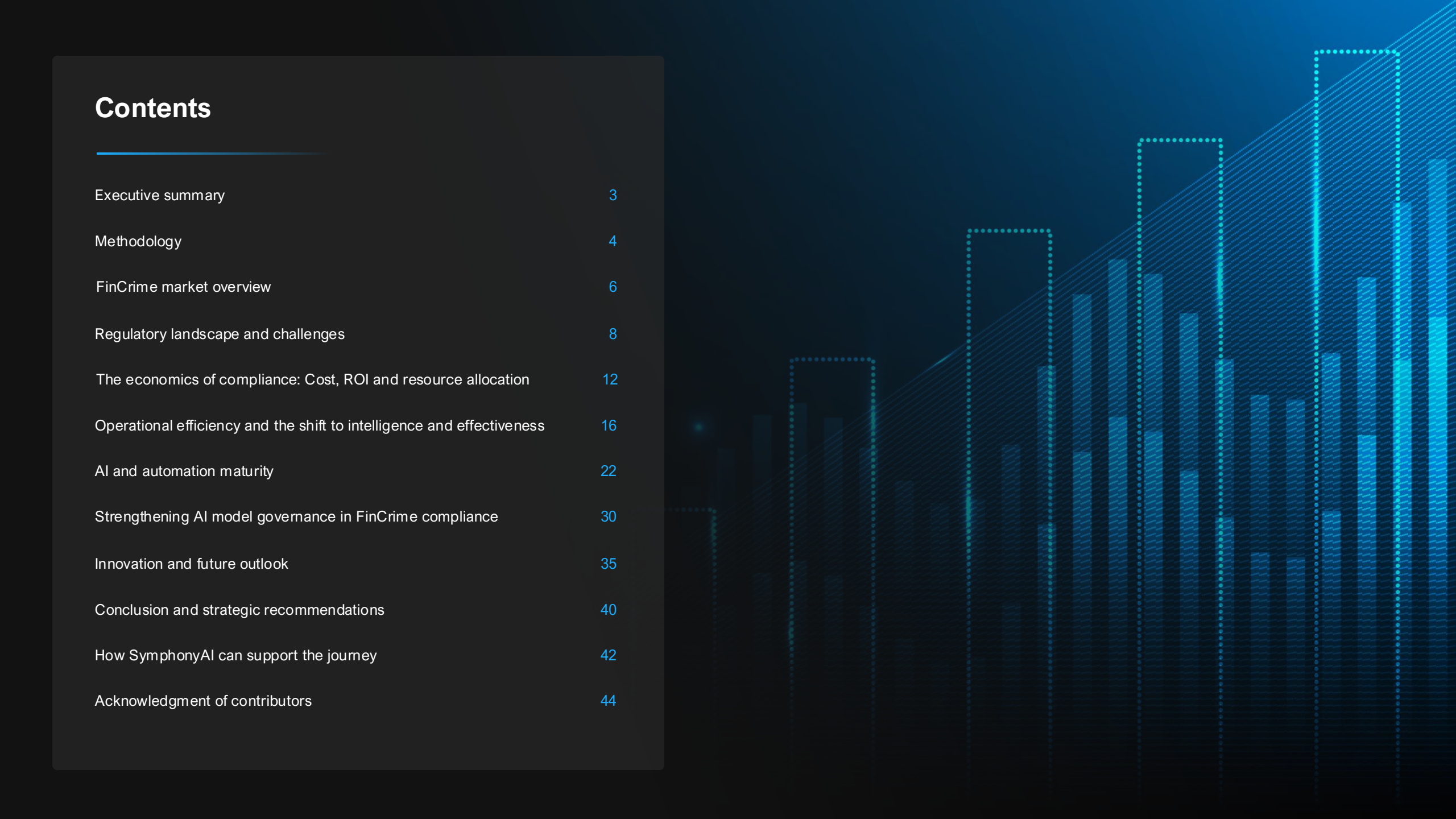
SymphonyAI | AML Intelligence

FinCrime Frontier 2025-26

The state of AI, regulation, and readiness in financial crime compliance

Contents



Executive summary

The financial crime compliance landscape in EMEA is undergoing a period of profound transformation.

As financial institutions navigate increasingly complex regulatory demands, a rapidly evolving threat landscape, and rising operational costs, the need for innovation, efficiency, and intelligence-led compliance has never been greater. At the same time, the rise of AI, particularly in screening, monitoring, and investigations is opening new frontiers in the fight against financial crime.

The **FinCrime Frontier 2025-26** survey was launched to capture a clear, data-driven view of how the industry is responding to this change. Over a six-week period, we gathered insights from compliance leaders, risk professionals, and AML specialists across the banking and insurance sectors in the EMEA and Americas regions. Their responses reflect a sector at a pivotal point, balancing regulatory expectation with transformation ambition.

Key findings include:

- **AI adoption is accelerating**, yet many institutions remain in the early stages and face ongoing and integration challenges.
- **The cost of compliance continues to rise**, with budget pressures impacting strategic investment decisions.
- **Model governance and regulatory scrutiny are now front-of-mind** as institutions embrace and scale their use of AI and automation.
- **A growing demand for deeper cross-industry collaboration**, clearer regulatory guidance, and access to shared intelligence.

This report offers a comprehensive snapshot of where the industry stands today and where it's headed next. From operational pain points to technology priorities, and AI transformation to cross-border regulatory trends, it captures the tensions, opportunities, and innovations defining the future of FinCrime prevention.

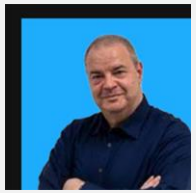
At **SymphonyAI Financial Services**, our mission is to empower compliance teams with trusted, AI-driven solutions that are not only innovative, but deeply aligned with the realities of regulatory risk and operational complexity.

At **AML Intelligence**, we are proud to support this initiative as part of our commitment to advancing financial crime journalism, regulatory transparency, and global collaboration between public and private stakeholders. By amplifying the voices of compliance professionals and bringing data-driven insights to light, we aim to contribute meaningfully to shaping policy, informing decision-makers, and supporting the fight against financial crime across jurisdictions.

We extend our sincere thanks to everyone who contributed to this research. We hope this report sparks new conversations and actionable change across the financial services ecosystem.

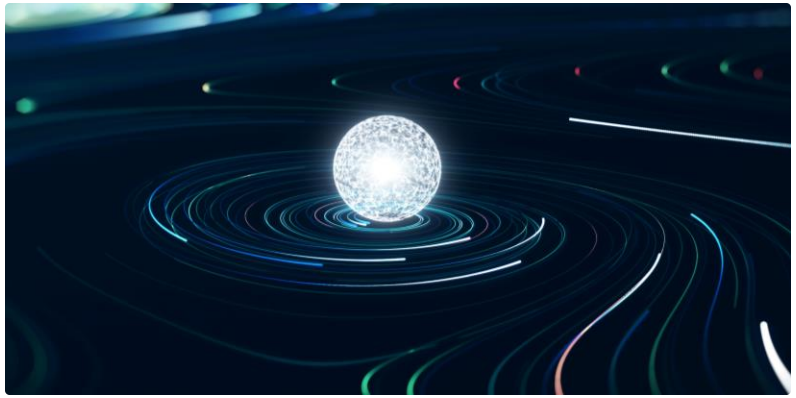
Stephen Rae

Co-Founder and Chair, AML Intelligence



Jason Shane

Head of Product Strategy and Innovation, SymphonyAI



Methodology

The FinCrime Frontier 2025–26 study was designed to provide a comprehensive health check on the state of financial crime compliance and innovation across global financial institutions. Its purpose is simple yet broad: to illuminate the most pressing challenges, priorities, and transformations shaping the future of compliance.

Conducted jointly by SymphonyAI and AML Intelligence, the study surveyed over 250 senior financial crime and compliance professionals across banking, insurance, and fintech sectors worldwide. The respondent base included senior executives, compliance officers, AML leaders, and risk and technology specialists, offering a comprehensive view of the industry's strategic direction and operational realities.

The survey, conducted between July 2 and August 31, 2025, captured both quantitative and qualitative insights through a structured 42-question online questionnaire. The questionnaire was distributed via SymphonyAI and AML Intelligence's communication channels and comprised primarily multiple-choice questions, with some open-ended fields to gather in-depth commentary and context from respondents.

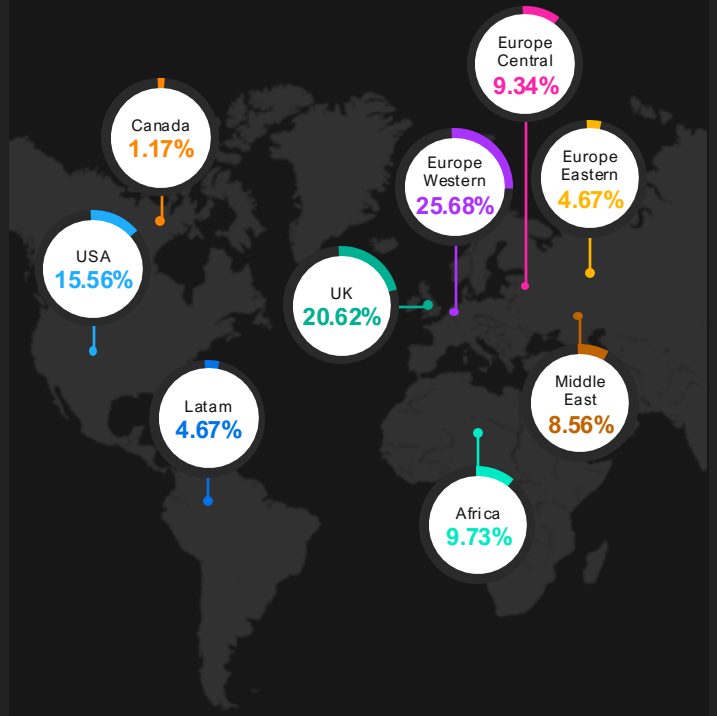
The survey explored four central themes:

- **AI and automation maturity** – How far institutions have progressed in adopting, governing, and scaling intelligent compliance technologies.
- **Regulatory readiness and challenges** – The evolving regulatory landscape and the financial and operational impact of AMLA, FATF, FinCEN, and other frameworks.
- **Operational efficiency and pain points** – Where institutions face the greatest barriers, from data quality to alert management and resource constraints.
- **Future innovation and investment priorities** – The industry's outlook on AI, automation, and collaborative approaches to financial crime prevention.

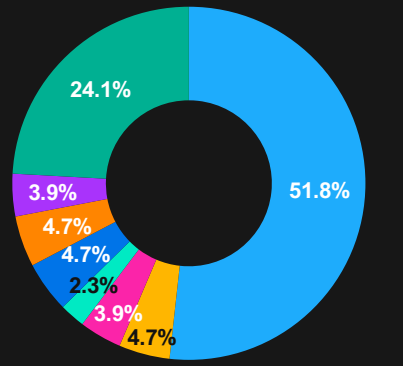
Together, these findings offer an evidence-based perspective on where the financial crime compliance sector stands today and where it is headed next. For decision-makers, FinCrime Frontier 2025–26 provides actionable intelligence on technology investment, governance practices, and regulatory preparedness, helping shape more resilient, AI-enabled compliance programs for the future.

Demographics

Respondents by region

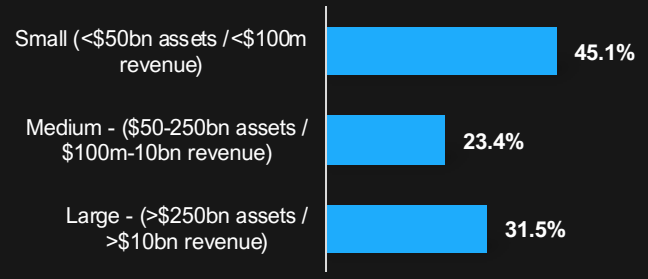


Type of organizations

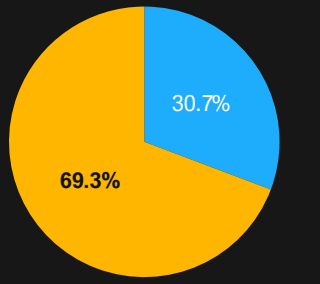


- Banking (including Capital Markets)
- Insurance
- Regulator
- Investment firm
- NBFI
- Professional Services
- Consultancy
- Other

Size of organizations

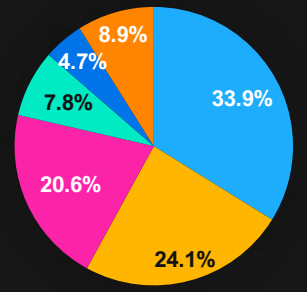


Respondents by Line of Defense (LOD)



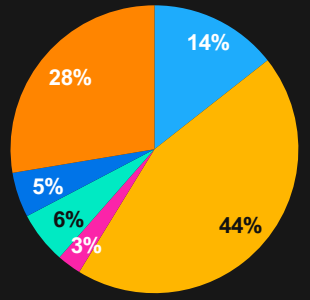
- 1LOD
- 2LOD

Respondents by job title



- Head of Function
- Team Manager/ Leader
- Team Member
- Process, Operations & Control
- Quality Assurance
- Other

Respondents by function



- KYC / CDD / EDD
- AML
- Sanctions
- Fraud
- Technology
- Other

FinCrime market overview

Effective compliance has become critical as financial crime threats and regulatory demands increase. Criminals are leveraging more sophisticated methods to exploit the global financial system. In response, regulators and financial institutions must adapt quickly or risk major systemic vulnerabilities. This chapter focuses on the current state of anti-money laundering (AML) regulation, operational practice, and technology within the financial services sector, and how these converge in the fight against financial crime.

Regulation in the AML space remains daunting.

In the Financial Action Task Force (FATF) jurisdictions, the regulatory agenda is intensifying. In Europe, the European Commission updated the list of high-risk third countries amongst other things, signaling tougher cross-border vigilance. Within the United Kingdom, the government published draft amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) in 2025, targeting loopholes and seeking to make due diligence more risk-based.

Meanwhile, in the United States (US) and Canada the picture is more mixed. Canada launched robust updates to its AML/ATF regime and rolled out new requirements effective October 2025, and the US under the Financial Crimes Enforcement Network (FinCEN), delayed the implementation date of a major AML rule for investment advisers from January 2026 to January 2028, signaling some regulatory breathing space.

The EU and UK:

The EU's new AML/CFT framework is underway and will come into full force in 2025-26. The newly created European Union Anti Money Laundering Authority (EU AMLA) assumed direct and indirect supervisory powers over high-risk entities (from July 2025) and will select their 40 to directly supervise shortly. In the UK, changes proposed by HM Treasury aim to take effect by end of 2025, including digital ID for KYC, proportionality in obligations, risk-based scrutiny, and revocation of certain assimilated EU laws.

In 2026, institutions can expect tighter enforcement, deeper cooperation across member states, stronger beneficial ownership regimes, and more regulatory technical standards (RTS) under the AML/CFT framework in the EU.

The U.S. and Canada:

In the US, despite heightened rhetoric on financial crime, some major rules have been delayed, such as the investment adviser AML/SAR rule will now likely go live in 2028.

At the same time, the US has signaled a tilt toward easing some compliance burdens in order to support business activity, raising concerns about potential exploitability by criminals. In Canada, regulatory momentum is strong. Amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) is set to increase penalties, widen reporting obligations, and tighten controls in 2025 and beyond. Canadian institutions should prepare for further regulatory tightening and enhanced international cooperation frameworks in 2026.

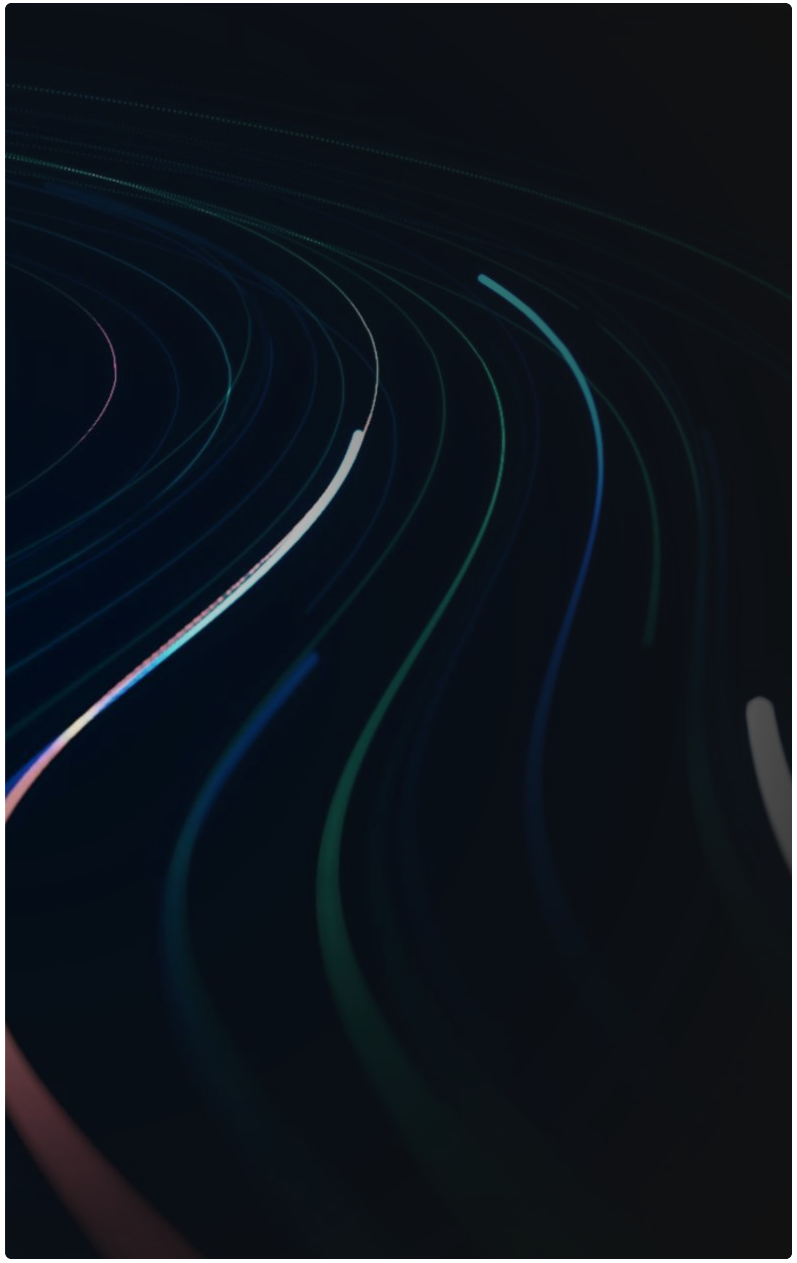
These contrasting approaches, tighter controls in Europe and more relaxation or delays in the US, create divergent regulatory regimes across geographies.

From an **operational perspective** within financial institutions, AML compliance functions remain challenged. Many organizations still rely on largely reactive frameworks, such as performance metrics focus on volume of alerts or investigations compared to an outcome-based prevention proactive approach.

Changes to policy and procedures are underway in response to impending regulation, but implementation often lags behind criminal innovation. The speed of threat evolution means many AML compliance programs struggle to keep up with the pace of change. Organizations are refining KYC, transaction monitoring, enhanced due diligence and beneficial-ownership processes to align with the new regulatory demands.

On the **technology front**, financial institutions are actively integrating advanced technology into their AML compliance functions. Many have begun planning for AI-driven analytics, real-time transaction monitoring, and knowledge graph frameworks to gain a comprehensive, connected view of customer behavior, transaction flows, and network relationships. These technologies enable faster identification of suspicious patterns and reduce false positives, allowing compliance teams to focus on higher-risk cases. AML Compliance functions are also investing in machine learning for dynamic risk scoring and automating case management workflows to accelerate investigations and regulatory reporting. Despite these advances, many organizations face challenges with legacy systems and fragmented data, prompting a growing trend towards cloud-based, modular AML solutions that can be layered over existing infrastructure with minimal disruption.

The technology outlook shows significant opportunity however, as confidence grows and evidence-based outcomes are realized faster. For example, organizations set to enhance their AI capabilities with explainable models for greater transparency and regulatory acceptance will see benefits from the implementations quickly. Automation maturity will deepen, with broader deployment of agentic AI architectures handling end-to-end compliance workflows, from customer onboarding to suspicious activity reporting. The future will also emphasize proactive intelligence, leveraging predictive analytics and behavioral insights to anticipate emerging threat typologies before they materialize.



Regulatory landscape and challenges

The regulatory environment for financial crime compliance is entering one of its most dynamic phases in over a decade. As institutions modernize their compliance frameworks, regulators across EMEA and North America are simultaneously expanding expectations demanding greater transparency, stronger governance, and demonstrable effectiveness.

The survey findings show that the **regulatory landscape and volume of change (26.2%)** rank as the second-largest concern among financial crime risks, following the **growing sophistication of criminal tactics and tools (41.8%).** This underscores a persistent challenge – keeping pace with evolving regulatory obligations remains a significant external pressure.

Institutions across both regions report that they are navigating a convergence of pressures – from complex, cross-border regulatory frameworks such as EU AMLA, the 6AMLD, and FinCEN's modernization initiatives, to emerging rules around beneficial ownership, operational resilience, and instant payments.

Data integrity, jurisdictional alignment, and the pace of regulatory change are defining themes shaping 2025–26 compliance strategies. Yet, respondents largely view regulatory evolution as a catalyst for modernization driving investment in stronger governance, automation, and RegTech integration. The challenge lies not in intent, but in execution: the frequency, depth, and quality of engagement with regulators remain uneven, indicating the need for a more proactive, technology-informed dialogue between compliance leaders and supervisory bodies.

As the regulatory bar continues to rise, financial institutions will need to embed adaptive, risk-based compliance frameworks that can evolve alongside policy and enforcement trends, balancing innovation with accountability, and transformation with control.

The next challenge for compliance leaders is not simply to interpret these requirements, but to operationalize them across real-time, data-driven, cross-border ecosystems.

When it comes to the biggest AML/ fraud regulatory challenges in 2025–26, responses can be categorized into four key fronts:

1. Real-time payments (RTP/ FedNow/ instant rails) and the shift from post-event to real-time monitoring/ reporting.
2. Cross-border complexity – divergent rules and data-sharing constraints across jurisdictions .
3. The EU package (EU AMLA/ AMLR/ 6AMLD) alongside FinCEN updates and FATF expectations, including sanctions updates and mutual evaluations.
4. Emerging-tech pressure – crypto/virtual assets, ISO 20022 migration, confirmation of payee, synthetic IDs/ deepfakes, and UBO transparency. Many also cite budget/ talent limits and legacy tech as obstacles to meeting these faster, tougher expectations.

Respondents most frequently cited **EU AMLA, 6AMLD, and RTP initiatives as the leading sources of compliance strain and investment pressure,** reflecting the growing complexity of aligning cross-border requirements with faster, data-driven financial ecosystems.

To keep pace, compliance programs will need to become real-time, cross-jurisdictional, and explainable. That means prioritizing streaming analytics and alerting, strong data governance and interoperability for cross-border use cases, and AI/ ML with auditability to handle fraud/ AML convergence and identity risk.

Navigating the patchwork of global AML regulations remains the most pressing challenge, cited by **nearly 57% of respondents** a clear indication that regulatory fragmentation continues to strain multinational compliance programs. Secondary pain points around data privacy, technology integration, and cost balance highlight the tension between innovation and regulatory constraint in cross-border operations.

High-impact regulations reshaping compliance operations

The survey findings indicate that recent and upcoming regulations have not only reshaped compliance priorities, but have also emerged as major cost drivers, influencing how financial institutions allocate resources, structure teams, and define return on compliance investment.

The largest financial impacts cluster around:

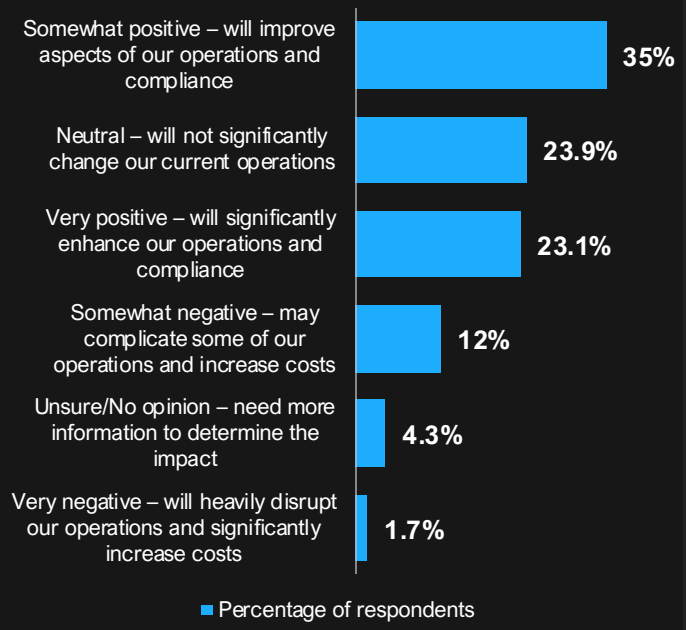
1. **EU AML package** (AMLA/ AMLR/ 6AMLD) and **FATF/ FinCEN updates**. These drive new and expanded reporting and EDD requirements, cross-border harmonization, and repapering/ UBO (CTA/ BOI) obligations – forcing data model changes, staff training, and added headcount.
2. **Sanctions expansion and sanctions operations.** Respondents cite sharp increases in screening scope, list churn, and investigations tooling, with sanctions compliance now rivalling AML in cost intensity.
3. **Real-time payments and ISO 20022 migration**. The move from batch to instant monitoring and the shift in payment message formats require system overhauls, streaming analytics, and 24/7 alert handling – significantly raising infrastructure and staffing costs.
4. **Crypto and digital-asset rules** (Travel Rule, MiCA)**, confirmation of payee, DAC8, DORA/ operational resilience, PSR, Companies House/ECCTA changes.** These add connectivity to external networks, new data retention and reporting standards, and strengthened resilience controls.
5. **Model governance and explainability requirements.** As AI becomes embedded in financial crime compliance, regulators increasingly expect auditable, transparent models – driving investment in model risk management, documentation, and validation frameworks.

Overall, the responses highlight an urgent need for harmonized frameworks, standardized data architectures, and unified oversight tools. Institutions that invest in real-time analytics and reusable controls such as a single UBO service supporting KYC, screening, and reporting, will be best positioned to absorb regulatory shocks and sustain operational resilience.

Regulatory evolution seen as a driver for modernization, not disruption

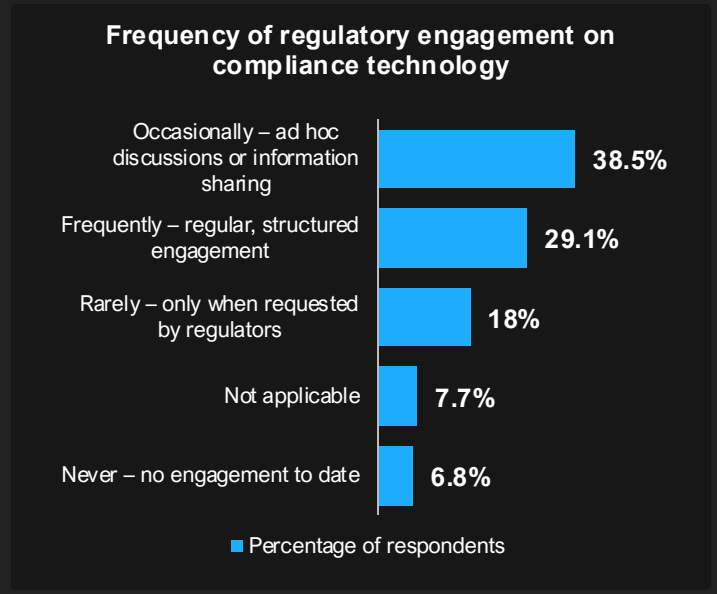
Despite the financial pressures, industry sentiment toward regulatory change remains broadly optimistic. A clear majority of respondents view upcoming regulations as an overall opportunity rather than a burden, **58%** describing the impact as positive (23% very positive, 35% somewhat positive). **24%** expect neutral effects, indicating that many institutions believe they're already well-aligned with regulatory trajectories. Only **14%** foresee negative consequences, mainly due to added complexity or cost, and a small minority (4%) remain uncertain.

Overall, the responses reflect a maturing compliance landscape. Most compliance leaders see regulatory change as a catalyst for modernization driving better data governance, technology investment, and stronger cross-border alignment. However, the minority warning of added costs and disruption underscores a growing execution gap: organizations that lag in automation, AI adoption, or data readiness may struggle to meet new compliance expectations on time and at scale.



From clarification to collaboration: the evolving regulator-institution dialogue

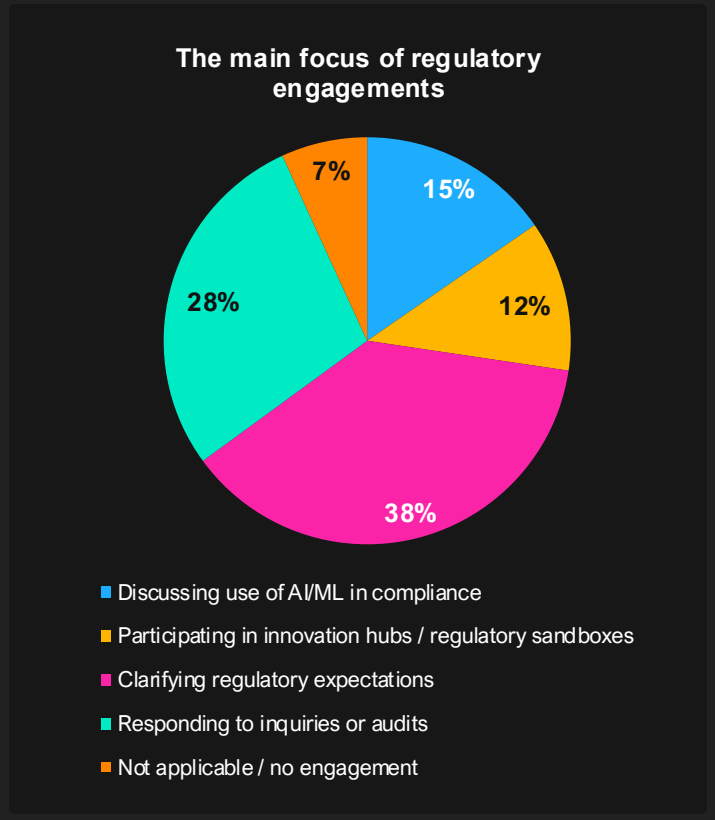
Regulator engagement on compliance technology and innovation remains limited and largely ad hoc. While **38.5%** of organizations report occasional, informal discussions with regulators, only **29.1%** maintain structured, regular engagement. Nearly **18%** engage only when prompted, and a combined **~14%** have little to no engagement at all.



These findings reinforce the previous results, confirming that most regulatory engagement remains reactive rather than collaborative. While earlier data showed that the majority of institutions interact with regulators primarily to clarify expectations or respond to audits, this question further reveals that structured, ongoing dialogue particularly around compliance technology and AI innovation is still rare.

As regulatory expectations evolve and technology adoption accelerates, organizations that build proactive, ongoing partnerships with regulators will be better positioned to help shape the frameworks governing next-generation compliance.

Most organizations' interactions with regulators remain reactive and clarification-driven, with **38%** engaging primarily to clarify regulatory expectations and **28%** responding to audits or inquiries. The comparatively lower engagement on AI/ ML discussions (15%) and participation in sandboxes (12%) reveals that while interest in advanced technologies is growing, formal regulatory dialogue around their use is still emerging.



The data suggests that while regulatory engagement is frequent, it is still dominated by compliance maintenance rather than collaborative innovation. Overall, these results reflect a transitional stage in regulator–institution relationships where oversight and assurance remain the priority, but momentum toward collaborative innovation and AI governance is steadily building.

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

How to embrace AI while managing regulatory requirements

As financial institutions accelerate AI adoption in compliance and financial crime prevention, the path to success depends on balancing innovation with control. Regulatory expectations may still be evolving, but the principles of responsible AI are already clear – institutions must demonstrate transparency, accountability, and explainability at every stage of the model lifecycle.

Start with strong governance
Establish clear roles, written policies, and accountability frameworks to ensure AI supports, rather than undermines, compliance objectives. Governance must extend across model ownership, approval, and ongoing validation.

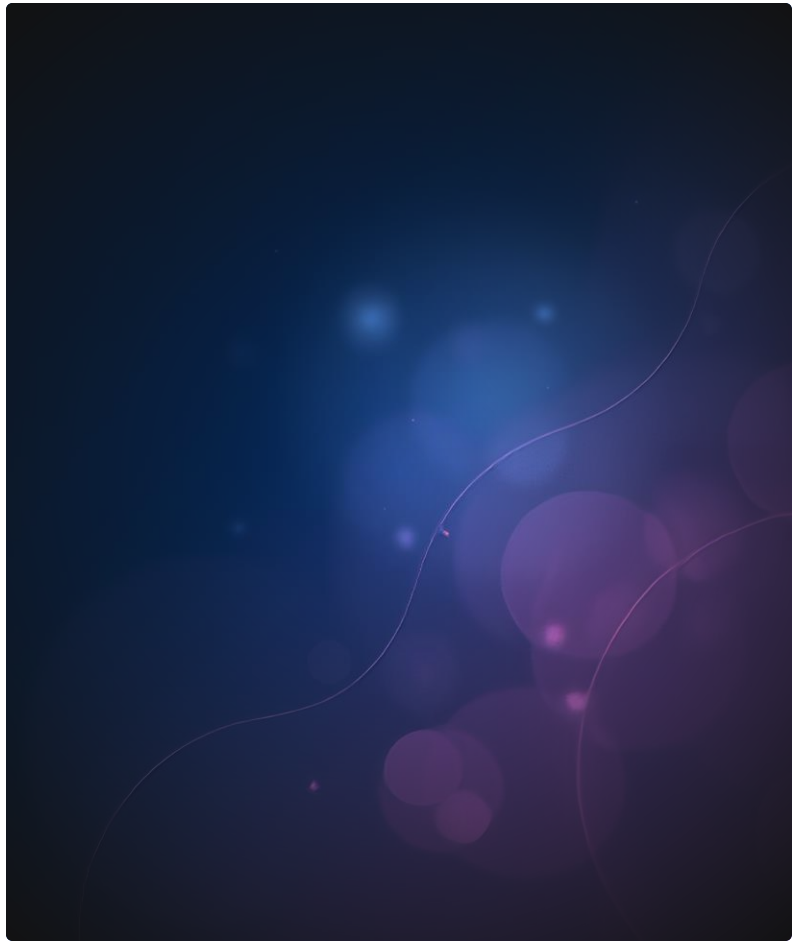
Document everything
Maintain a transparent and shareable record of how AI models are designed, trained, monitored, and updated.

Engage regulators early
Open, proactive dialogue with regulators helps shape future expectations and demonstrates readiness. Institutions that explain how AI enhances risk management will find regulators more receptive to its responsible use.

Data quality is critical
AI effectiveness depends on the integrity of the data powering it. Clean, bias-tested data, supported by lineage tracking and continuous audits, ensures accuracy, fairness, and defensibility.

Explainability and human oversight matter
If a model's decisions cannot be explained, it should not be deployed in compliance workflows. Human-in-the-loop oversight combined with sandbox testing remains essential to ensure ethical, accountable AI use.

The future of AI in financial crime prevention will favor organizations that combine innovation with discipline – treating AI not as a "black box" solution, but as a transparent, auditable, and well-governed partner in compliance.



The economics of compliance: cost, ROI and resource allocation

Despite economic pressures, compliance leaders are doubling down on technology modernization and data integration, indicating a clear shift from capacity growth to capability building.

Tech enablement

AI integration

Automation

Over 2025–26, investment priorities concentrate on technology enablement, AI integration, and automation of manual workflows.

Data quality and access have become critical enablers, reflecting the industry's push for smarter, faster, and more accurate compliance operations.

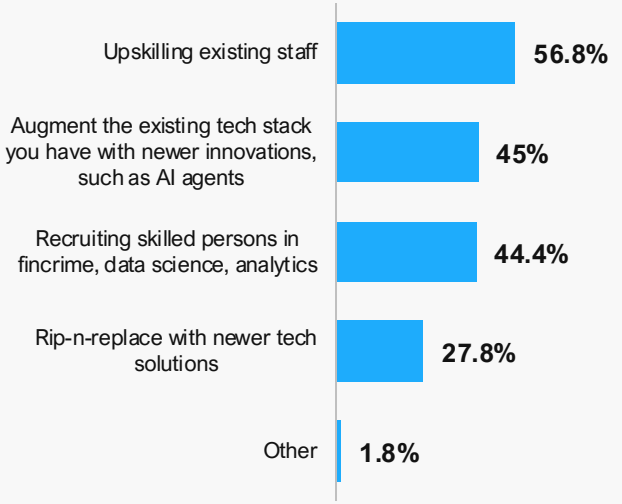
The emphasis is moving from 'more people' to 'better systems.' Institutions are consolidating tools, deploying AI overlays, and using automation to reduce address known pain points, such alert fatigue and investigation time. While staffing and training remain important, growth here is targeted toward reskilling teams for data-driven, tech-augmented roles.

Spending priorities: building capability over replacement

When it comes to spending priorities to maintain or improve operational effectiveness, the data reflects a measured, capability-driven strategy rather than radical overhaul.

- **56.8%** plan to upskill existing staff, recognizing that human capability remains central to managing evolving regulatory and technological complexity.
- **44%** are investing in specialized talent across compliance, such as data scientists and analytics experts. This underscores the growing demand for hybrid talent – professionals who combine deep compliance expertise with strong technological fluency.
- **45%** intend to augment their existing tech stack with new tools such as AI agents, workflow automation, and data enrichment solutions rather than replace it entirely.
- Only **27.8%** are pursuing "rip-and-replace" modernization, highlighting budget caution and dependency on legacy systems as reasons to hold back.

Planned areas of investment for compliance effectiveness



Multiple responses permitted; percentages may exceed 100%.

> "We focus on a hybrid model that combines in-depth staff development with the continuous refinement of proprietary technologies, balancing human expertise with system optimization."

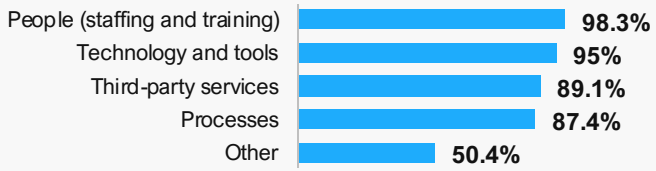
Together, these insights confirm that financial institutions are moving toward incremental modernization and human capability building. Most institutions remain mid-journey in their automation of financial crime compliance. Those that integrate automation with data, explainability, and human expertise will move ahead fastest.

A balanced investment model

Survey findings show that compliance teams are investing broadly across various areas to build more resilient, data-driven operations:

- **98%** of respondents allocate significant resources to people: staffing, training, and upskilling remain top priorities, even as automation advances.
- **95%** invest in technology and tools, underscoring the continuing shift toward modernization and AI-enabled detection and monitoring.
- **89%** rely on third-party services, while **87%** emphasize process improvement initiatives aimed at workflow optimization and control efficiency.

Compliance budget allocation by category



Multiple responses permitted; percentages may exceed 100%.

This balanced allocation highlights a maturing compliance function that views investment in people and platforms as complementary not competing priorities. The goal is a hybrid model where technology amplifies human expertise rather than replaces it.

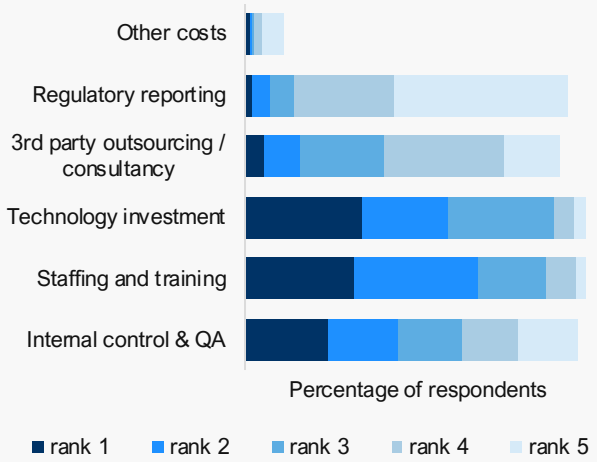
Technology and talent: the twin cost pressures

When ranking areas of highest cost impact, respondents identified technology investment (34.7%) and staffing and training (31.4%) as the two dominant cost drivers. Internal controls and quality assurance (24%) follow closely, reflecting the ongoing effort to maintain accuracy and audit readiness across fast-changing programs.

By contrast, outsourcing and consultancy (35.5%) and regulatory reporting (52.1%) dominate the lower cost tier. This suggests a clear industry trend toward self-sufficiency, with more institutions building internal expertise and developing proprietary compliance infrastructure instead of depending heavily on external advisors.

The results point to an industry in transition toward self-sufficiency and modernization. Financial institutions are building in-house expertise while investing in next-generation compliance technology. However, these same areas. i.e. people and platforms are also the most resource-intensive, reinforcing the need for better alignment between spending and measurable outcomes.

Greatest cost impact on compliance functions (ranked 1-5)



Balancing transformation with cost discipline

The findings reveal a clear dual challenge: institutions must modernize to remain compliant while maintaining cost discipline.

Automation, AI, and data modernization now sit at the core of most investment strategies, yet upskilling staff to manage and interpret these technologies remains equally essential.

To balance innovation with efficiency, leading organizations are:

- Aligning technology spend with measurable outcomes, such as reduced false positives and faster case resolution.
- Automating internal controls and quality assurance to reduce manual overhead.
- Leveraging AI to personalize training and enhance risk-based quality assurance.

This shift marks a strategic inflection point - the cost of modernization is recognized an investment in long-term sustainability and efficiency, rather than a business expense.

Future cost efficiencies: automation and AI take the lead

Looking ahead, most institutions expect the **greatest cost savings in the next two years to come from automation and AI adoption,** particularly in:

- Transaction monitoring and alert management
- Sanctions screening
- KYC/CDD and onboarding processes

Respondents see automation as a direct lever for cost reduction cutting manual reviews, minimizing false positives, and freeing analysts to focus on higher-risk, higher-value investigations.

Many anticipate further staffing efficiencies, as automation reduces reliance on large analyst teams while boosting productivity through smarter tools and targeted training.

Others highlight secondary savings in training, investigations, and quality assurance practices, as technology streamlines workflows and eliminates duplication.

AI-driven automation is expected to deliver the most meaningful cost efficiencies allowing compliance teams to focus on higher-value, risk-based activities.

ROI measurement: a critical gap

The return on investment (ROI) in compliance is found by assessing gains from reducing risk and enhancing performance relative to the sum of all expenditures on workforce, operational processes, technology and tooling.

Despite rising investment, ROI analysis remains largely overlooked in compliance technology spending.

- **72%** of respondents have not conducted a formal ROI assessment.
- Only **28%** have done so, typically as part of broader digital transformation programs.

This gap suggests that technology adoption remains largely reactive, driven by regulatory necessity, rather than a measured evaluation of financial impact. The absence of standardized ROI tracking continues to limit institutions' ability to quantify productivity gains, enhanced risk coverage, or cost savings.

However, momentum is shifting. As AI integration accelerates, more institutions are introducing ROI frameworks anchored in operational activities.

More institutions are establishing ROI frameworks tied to **operational KPIs**, such as:

- False-positive reduction
- Case resolution time
- Detection accuracy
- Cost per investigation or alert

These emerging metrics mark a clear move toward performance-based compliance management.

Guidance for compliance budget owners

Compliance investment is entering a new performance era. The next generation of compliance leaders will combine ROI discipline, hybrid talent, and purposeful modernization to achieve sustainable, high-performance operations in 2026 and beyond.

1. **Shift from spend to return**
   Embed ROI tracking into every major compliance investment. Link technology spend to measurable performance outcomes such as reduced false positives, faster investigations, and lower operational overhead.

2. **Invest in the human-machine partnership**
   Prioritize reskilling and redeploying staff for technology-augmented roles. Human judgment, contextual insight, and ethical oversight will remain essential as automation scales.

3. **Modernize with intent, not volume**
   Avoid fragmented tool portfolios. Focus budgets on integration, data quality, and workflow orchestration to maximize the value of existing infrastructure.

4. **Reframe compliance as a productivity engine**
   Position compliance as a driver of institutional intelligence. Demonstrate efficiency, accuracy, and resilience gains that strengthen both regulatory readiness and business value.

Operational efficiency and the shift to intelligence and effectiveness

The FinCrime Frontier 2025–26 findings reveal that many organizations remain trapped in cycles of operational inefficiency, primarily due to manual processes and workflows, fragmented data, and legacy technology.

These persistent barriers keep teams reactive, meaning they struggle with slow processes, frequent manual interventions, and data silos that hinder real-time compliance and risk management. Factors such as poor data quality and resources constraints contribute to staff spending valuable time on repetitive tasks, leaving little capacity for strategic analysis and proactive intervention.

These inefficiencies are particularly evident in AML and sanctions programs, where disconnected systems and legacy infrastructure restrict visibility, impact effectiveness and slow the pace of modernization. Minimizing these gaps requires organizations to pursue automation maturity and technology readiness across their compliance operations.

Manual processes and operational bottlenecks

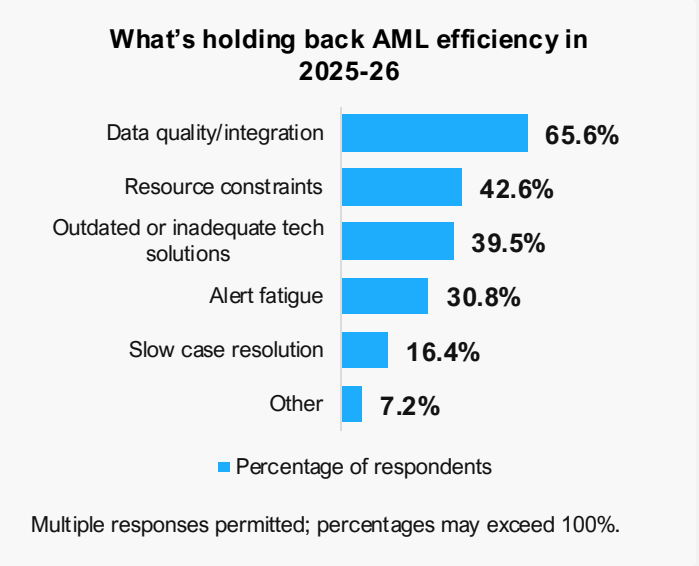
The survey reveals that the most manually intensive areas continue to be **Know Your Customer** (KYC), **Customer Due Diligence** (CDD/EDD), **onboarding, transaction monitoring,** and **Suspicious Activity Report** (SAR) drafting. These functions depend heavily on fragmented systems, inconsistent data, and extensive documentation. These factors mostly perpetuate inefficiency and increase the risk of human error.

Across respondents, many compliance teams still rely on manual data gathering and spreadsheets, consuming valuable analyst time on false positives instead of real risk. Investing in data integration, workflow automation, and AI-assisted triage can eliminate these manually intensive tasks. The shift from manual effort to intelligent automation isn't just about efficiency – it enables speed, control, and confidence in compliance operations.

The true barriers to AML efficiency

The biggest AML efficiency blockers are **data and workflow-related** – not regulatory uncertainty.

The single biggest drag on AML performance remains poor data quality and integration, cited by nearly **two-thirds (65.6%)** of respondents. It's a striking paradox: compliance programs are more data-driven than ever, yet many still lack unified, reliable data foundations. Inconsistent information across client profiles, transactions, and alerts continues to undermine both analytical accuracy and operational throughput.



Other major pain points compound the challenge. Resource constraints (42.6%) and outdated or inadequate technology (39.5%) limit scalability as transaction volumes and regulatory complexity grows. Alert fatigue (30.8%) drains analyst productivity, while slow case resolution times (16.4%) reveal persistent bottlenecks in investigations and escalation workflows.

True efficiency gains won't come from automation alone but from fixing the foundations – data integrity, modern infrastructure, and optimized teams. Institutions that address these core enablers will firstly achieve greater effectiveness, and secondly unlock faster investigations, higher analytical accuracy, and stronger regulatory assurance.

These results reinforce a critical dependency chain:

Data quality → **Technology enablement** → **Operational efficiency and effectiveness**

To address these issues, institutions should prioritize:

- Data standardization and integration across systems to reduce noise and duplication
- AI-enabled triage and prioritization to manage alert fatigue and accelerate case resolution
- Augmentation, not replacement, of teams using automation to free skilled investigators for higher-value analysis

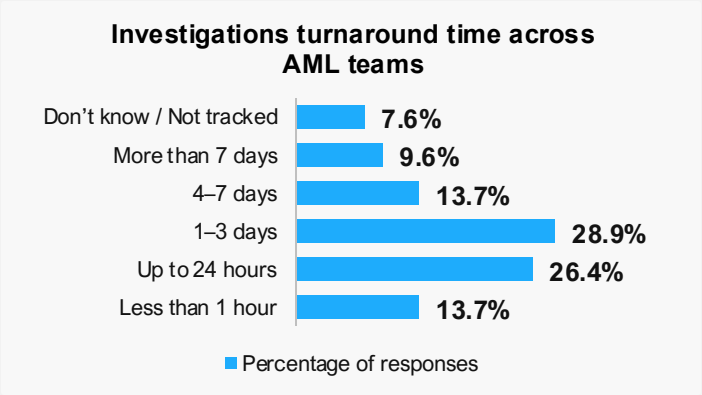
Investigation timelines: efficiency gains, but persistent variability

Investigation timelines remain highly uneven across financial institutions. A majority of respondents report resolving alerts **within 24 hours to three days,** reflecting moderate operational efficiency.

Yet nearly a quarter still take **four days or longer** to close cases, highlighting persistent bottlenecks and the complexity of multi-jurisdictional investigations.

A smaller, more advanced group (13.7%) achieve sub-hour resolution, typically leveraging automated triage and rule-based decisioning for low-risk alerts. Conversely, 7.6% of institutions admit they do not track investigation times at all – an indication of gaps in performance oversight and operational visibility.

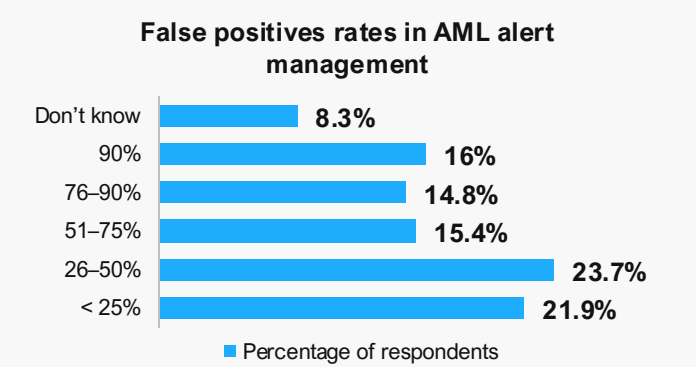
A clear maturity gap is emerging in AML investigations. Institutions with automated, centralized case management are achieving near-real-time resolution, while those reliant on manual reviews continue to face backlogs and limited visibility. As regulators tighten expectations around timely suspicious activity reporting, slow investigation cycles now represent both an efficiency gap and a compliance risk.



False positives: the core efficiency drain

High false positive rates remain one of the most persistent obstacles in AML operations. **More than 70%** of institutions report rates above 25%, and **nearly a third** face levels exceeding 75%, a costly drain on investigative resources. Only **one in five** organizations manage to keep false positives below 25%, while **16%** say that up to 90% of alerts are ultimately dismissed without action.

Perhaps most concerning, **8.3%** of respondents admit they do not track their false positive rate, highlighting weak performance monitoring and limited visibility into operational efficiency.



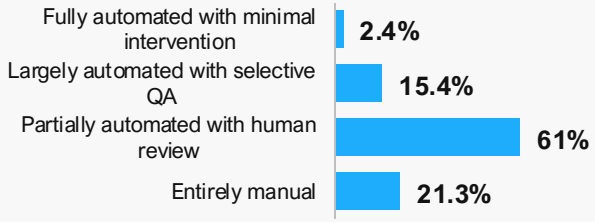
Persistent false positives reveal a structural flaw in traditional AML systems. Legacy rule-based models

flood teams with low-value alerts, while limited data enrichment prevents meaningful prioritization. Institutions adopting AI-driven triage, contextual analytics, and continuous model tuning can sharply reduce false alerts achieving faster risk response, lower costs, and greater operational focus.

Alert review models: the human–machine balance

Most institutions (61%) operate with partially automated workflows supported by human review – a hybrid model that reflects growing trust in technology but continued reliance on human judgment.

A significant minority (21.3%) still depend on fully manual reviews, underscoring the persistence of legacy processes. Meanwhile, only **15.4%** report largely automated workflows with selective quality assurance, and just **2.4%** have reached near-full automation with minimal human intervention.

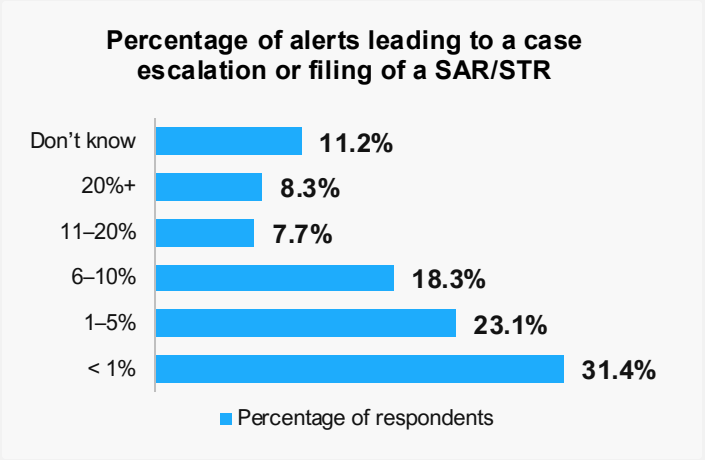


This finding underscores that, while automation is advancing, human judgment remains the cornerstone of alert management. The continued reliance on manual intervention reflects ongoing trust and explainability challenges, particularly in regulatory environments that demand full transparency and accountability.

A new model is emerging – **tiered alert review frameworks,** where automation handles low-risk, repetitive alerts, while investigators concentrate on complex, judgment-driven cases.

> The next frontier lies in optimizing human-technology collaboration. Using AI to amplify expertise, rather than replace it. When properly governed, this collaboration delivers faster, more consistent, and more explainable outcomes.

Yet despite progress, alert management remains one of the most stubborn bottlenecks in AML operations. The survey shows a stark imbalance between alert volume and investigative yield: **54%** respondents say that fewer than 5% of alerts lead to case escalation or SAR/STR filings, while **nearly a third (31%)** report conversion rates below 1%. Only **16%** of institutions achieve escalation rates above 10%.



Low alert-to-case conversion rates expose a core efficiency gap in AML operations. The underlying drivers are fragmented data, legacy detection logic, and limited feedback loops between investigators and model developers.

Institutions adopting risk-based triage, AI-driven alert scoring, and continuous model refinement are breaking this cycle – achieving higher accuracy, lighter workloads, and stronger compliance performance.

The next generation of AML programs will be defined by this shift: f**rom reactive investigation to proactive, intelligence-led detection**.

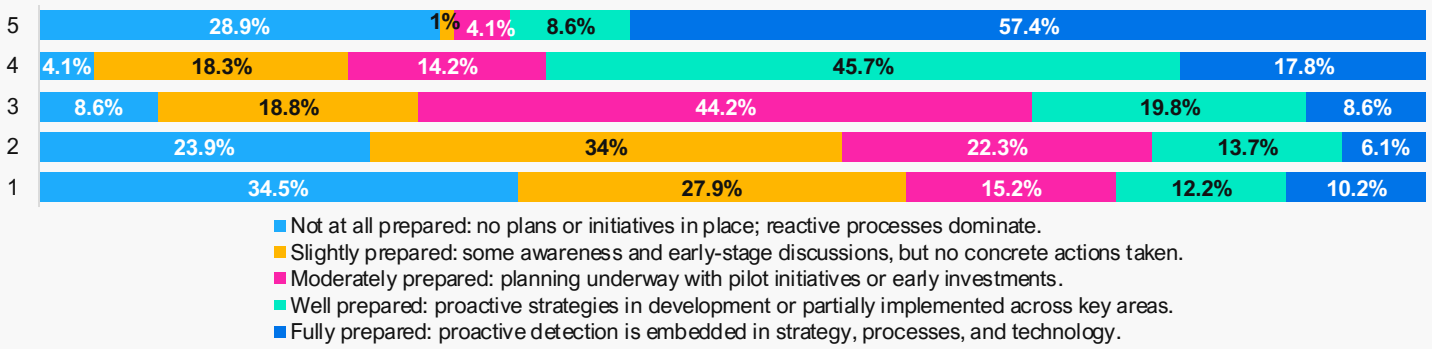
From reactive to proactive: shifting the detection mindset

The industry's long-standing dependence on rule-based, retrospective monitoring is rapidly giving way to predictive, intelligence-led models that identify risk earlier and adapt to new typologies in real time. Yet the transition remains uneven and cultural as much as technical. Progress depends on modern systems, though also on organizations' willingness to rethink how compliance intelligence is applied and acted upon.

The survey reveals a sharp disparity in readiness for proactive financial crime detection. While **57.4%** of respondents say their institutions are fully prepared to embed predictive models and analytics into compliance strategies, many remain in early stages of maturity.

More than a third (34.5%) admit they are not at all prepared, still operating reactively, and **27.9%** describe themselves as only slightly prepared, reflecting limited awareness or planning. Among those identifying as moderately prepared (44.2%), many are running AI or analytics pilots, indicating strong intent but uneven execution.

Readiness to shift from reactive to proactive financial crime detection (1-5 scale)



Multiple responses permitted; percentages may exceed 100%.

The readiness gap underscores the fragmented pace of progress across global financial crime compliance. Leading institutions are already deploying AI-powered monitoring, behavioral analytics, and network-based intelligence, while others remain hindered by legacy systems, fragmented data, and under-resourced transformation programs.

Automation and technology readiness

Most institutions continue to operate within the constraints of legacy systems, complex integrations, and cautious regulatory oversight, all of which temper the pace of change.

Across AML programs, automation levels remain limited and unevenly distributed.

- 38.5% of respondents report 26–50% automation
- 33.1% say 0–25% of processes are automated
- Only 21.3% have reached 51–75%, and just 7.1% report more than 75% automation.

70%

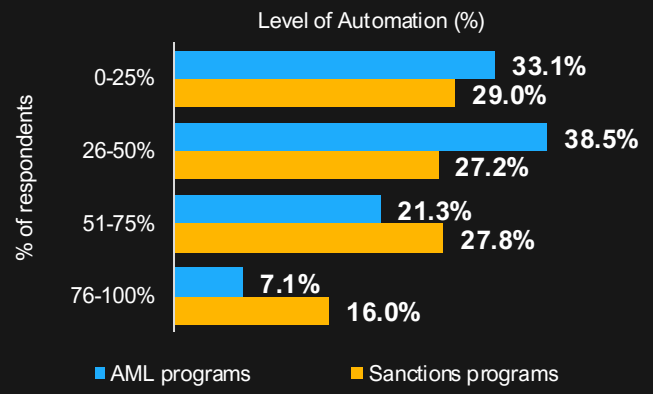
These results show that **over 70% of institutions still rely on manual operations for at least half of their AML activities.**

As revealed earlier in this report, **transaction monitoring**, **alert management**, and **SAR reporting** remain the most manual points in the AML lifecycle. These processes
are still heavily dependent on human judgment and narrative documentation despite growing automation.

By contrast, sanctions compliance appears moderately more advanced, though still short of full automation:

- 28.9% report 0–25% automation
- 27.2% fall within 26–50%
- 27.8% report 51–75%
- 16% have reached 76–100%

Comparison of automation levels: AML vs. sanctions programs



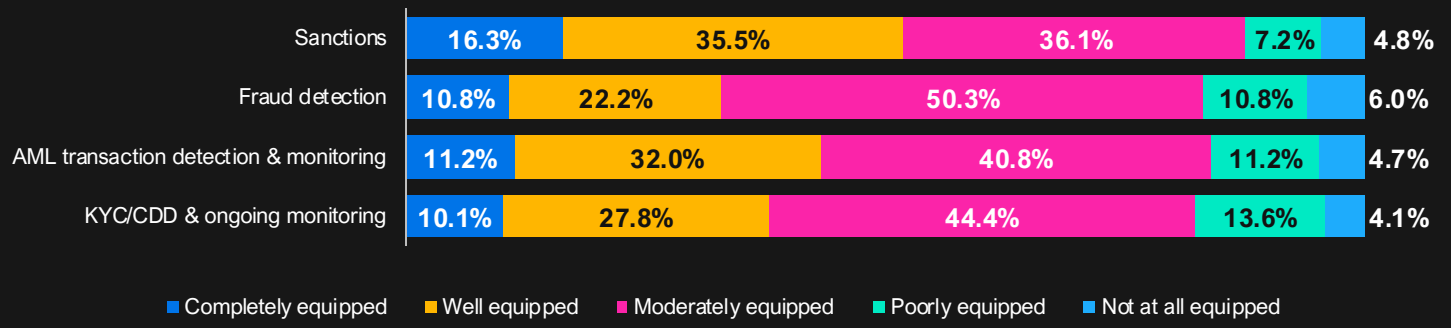
This more balanced distribution reflects that sanctions workflows, particularly name screening, fuzzy matching, and watchlist management lend themselves more easily to automation than investigative AML processes. Overall, **43%** of respondents have automated more than half of their sanctions programs, compared to just **28%** in AML underscoring both progress and persistent gaps in technology maturity.

Technology readiness: moderately equipped, but not future-proof

When asked how well-equipped their current technology stacks are to meet future regulatory expectations, most respondents placed themselves in the moderate readiness range indicating capability, but not confidence.

- Across all functions, 36–50% describe their systems as moderately equipped.
- Sanctions compliance leads the field, with 52% saying their systems are well or completely equipped.
- In contrast, only 38% say the same for KYC/CDD, and 43% for AML transaction monitoring.
- Fraud detection is the weakest area: just 33% rate their systems as well-prepared, while more than 60% classify them as moderate to poor.

Technology readiness across key compliance functions



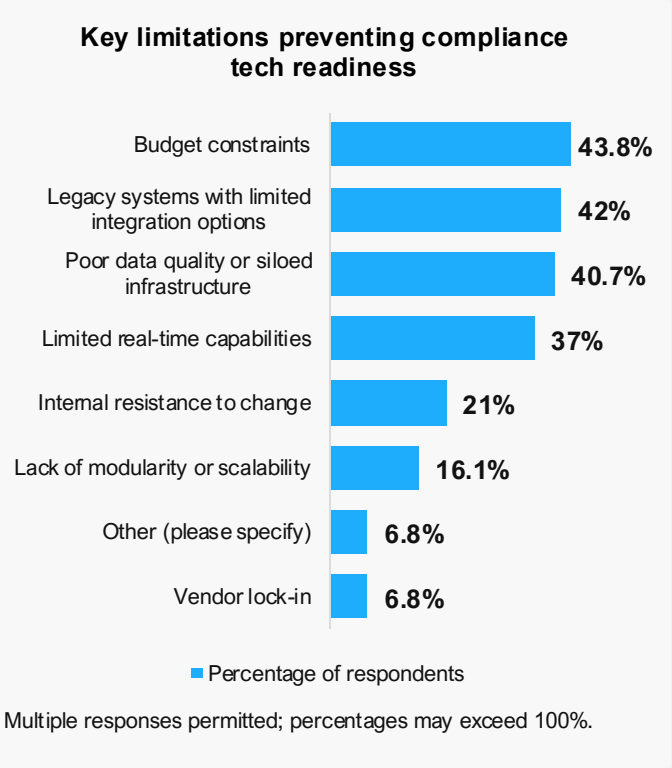
Although only a small minority (4–6%) of respondents said their systems were not at all equipped, the data points to a significant readiness gap, particularly among institutions managing multiple regulatory frameworks or legacy infrastructures.

While technology modernization is clearly underway, most compliance systems remain ready for today's demands rather than tomorrow's challenges. Institutions continue to balance regulatory compliance, cost, and integration complexity, slowing progress toward true future-readiness.

Barriers to future-readiness: legacy, budgets and data

Among institutions that reported being underprepared for future regulatory and operational demands, the top three limitations were:

- Budget constraints (43.8%)
- Legacy systems (42%)
- Poor data quality or siloed infrastructure (40.7%)



Other notable challenges include limited real-time capabilities (37%), internal resistance to change (21%), and scalability issues (16%) reflecting the structural inertia that continues to slow transformation.

> “The primary limitation is not a lack of technology, but the constantly growing complexity and pace of change in the external environment. This requires continuous effort in adaptation and data integration, even with an advanced tech stack.”

These findings reaffirm a familiar reality: the biggest barriers to modernization aren’t purely technical, they are financial and cultural. **Budget constraints, legacy systems, and poor data** integration continue to limit progress, leaving most institutions aware but underprepared. Readiness is improving, but true resilience remains a work in progress.

Achieving true efficiency will require a strategic shift – **from tactical automation to integrated intelligence.** Compliance leaders should focus on three priorities:

- Strengthen data integration to enhance accuracy and speed
- Deploy explainable AI to reduce false positives and accelerate case resolution
- Invest in hybrid skills that unite human judgment with machine precision.

The institutions that act on these imperatives will move beyond operational efficiency to achieve intelligence-led compliance.

AI and automation maturity

AI innovation in FinCrime functions has significantly advanced, transforming how organizations detect, prevent, and respond to illicit activities.

On a technical level, advanced machine learning models lead the tech-charge, from enhanced predictive models, to generative AI assist models, and now the agentic AI move with AI agents. The techniques enable real-time monitoring, scoring, and the automation of simple and connected compliance tasks, significantly reducing the impact of known pain-points and lowering operational costs.

From a business perspective, organizations gain agility, operational resilience, and competitive advantage through AI-powered tools that enhance detection accuracy, streamline workflows, and drive a new level of effectiveness in compliance programs.

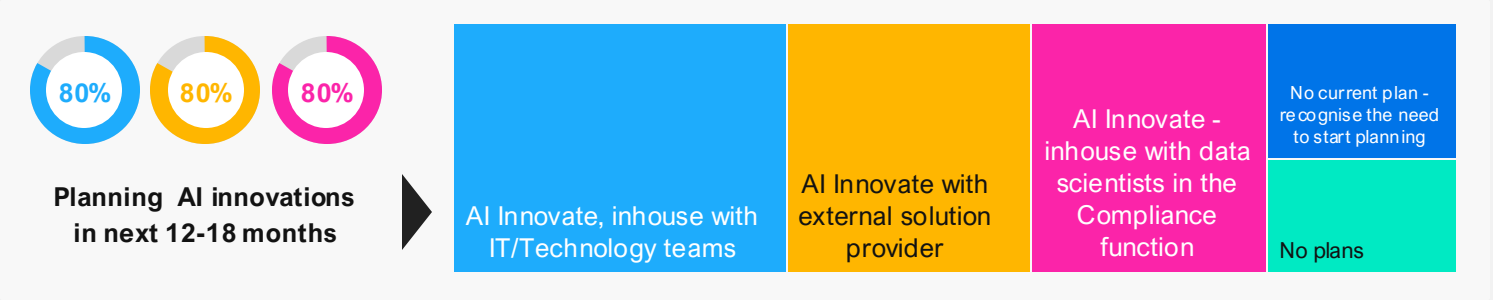
The performance benefits are being realized: many organizations report a two- to fourfold increase in crime detection rates and a substantial reduction in manual workload, enabling teams to move from reactive defense to proactive intelligence with strategic risk mitigation built-in.

As AI adoption matures, organizations increasingly leverage AI-driven insights for faster decision-making and more optimized resource allocation, marking a pivotal shift in financial crime compliance capabilities.

AI's role in compliance

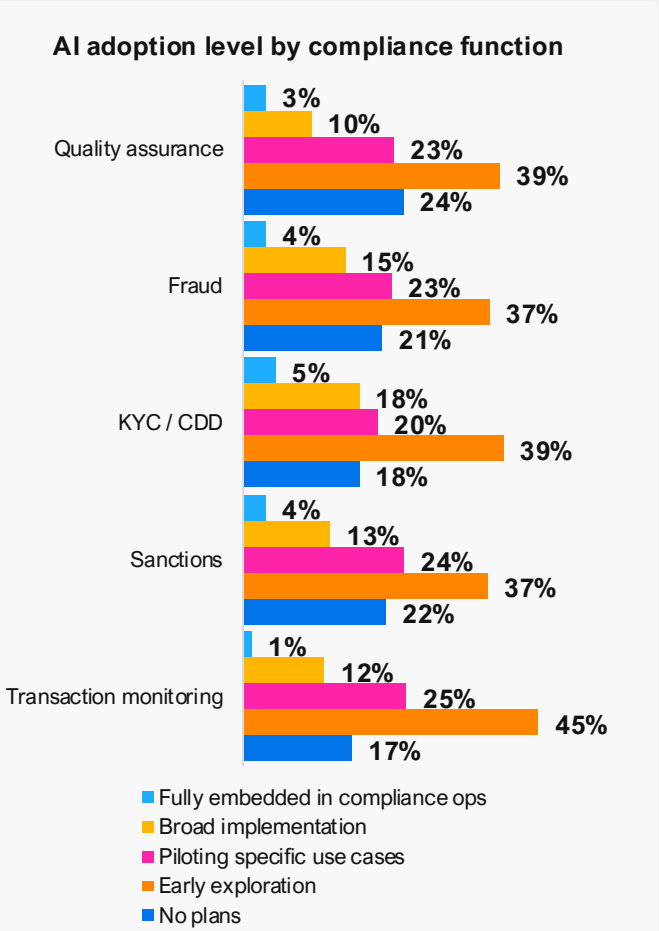
AI's role has shifted in the last two years - from older style machine learning techniques and analytics, to newer predictive and generative models - offering continuous detection of known and new threats, automation and advanced behavioral analytics to accelerate productivity and proactive risk management.

Early adopters of AI in financial crime functions continue to be the first to experience the benefits of AI, though the gap is closing. **80%** of respondents **plan to innovate with AI in the coming 12-18months**, either with in-house IT teams, a solution provider, or with their own compliance data science teams. 10% have not started planning yet though recognize the need to innovate in the near future, while the remaining 10% have no defined plans or budget secured to do so.



Growth on the horizon: the AI adoption landscape

There is a clear correlation between understanding how AI can be used in financial crime prevention and financial institutions' adoption rates of such technologies, evidenced by the fact that as comprehension of AI's capabilities deepens, proof of concepts (POC) and implementation grows.



Survey results indicate that most compliance functions are still in the early exploration or pilot phases of their AI adoption journey.

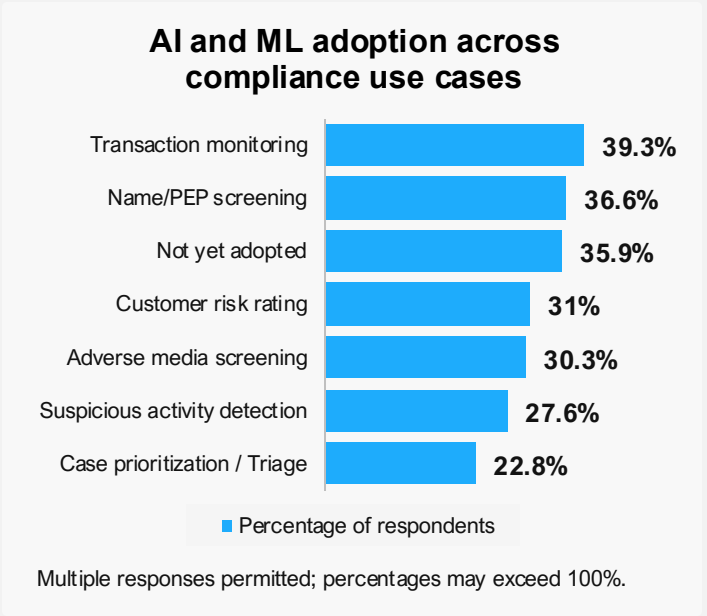
- Approximately **40–45%** of respondents are in the early exploration phase, experimenting with data, governance, and small-scale proof-of-concept projects.
- Another **20–25%** are piloting specific use cases, such as AI-assisted alert triage, sanctions screening optimization, or automated quality assurance (QA).
- However, only **10–17%** report broad implementation, and fewer than 5% say AI is fully embedded in compliance operations.

Transaction monitoring appears to lead slightly in early experimentation (45%) but lags in embedding, while **KYC/CDD** shows the most balanced progress, with a small but growing proportion (5%) achieving operational integration.

This pattern highlights that AI in compliance is moving from intent to action, but maturity remains limited for now.

Productivity and automation are key drivers of AI implementation and success. Both speed up processing and real-time outcomes, such as transaction screening and alert handling, allowing organizations to manage large volumes efficiently and reduce human error. This leads to fewer false positives, and faster, more accurate investigations, letting compliance teams focus on complex cases and improving overall risk management.

The early adopters of AI implementations are the first to see these benefits, with further follow-on POCs considered leading to implementations. Of those surveyed (where multiple answers were allowed), a relatively even distribution have implemented or piloted AI innovations to date across Transaction Monitoring (18%), Name/PEP Screening (16%), Adverse Media (14%) and Customer Risk Scoring (14%). The same percentage (16%) however have not yet adopted AI in financial crime solutions. This widespread speaks to the priority organizations are giving to solving certain pain-points first with AI innovations, to achieve a productivity or efficiency benefit.



Multiple responses permitted; percentages may exceed 100%.

Regarding the current use of AI in compliance programs, the majority of respondents expect to see a return on investment (ROI) from AI-driven compliance programs **within 12 to 24 months** after implementation, with some citing shorter windows (as little as 6–12 months) and others anticipating longer horizons of up to three years, depending on organizational maturity and integration complexity. The two most frequently mentioned areas for realizing ROI is **transaction monitoring** and **KYC/CDD**. A smaller group expects returns in fraud detection, regulatory reporting, and staffing efficiency.

Survey top themes on the use of AI in compliance program and ability to realize ROI		
35%	Transaction Monitoring	Often tied to reduced false positives, faster alert review, improved detection
24%	KYC / CDD / EDD/ Onboarding	Seen as a major source of efficiency gains (automation, faster onboarding, reduced manual labor)
10%	Efficiency / Process Automation (general)	Covers reduction in manual workload, operational streamlining, headcount savings, regulatory reporting
8%	Sanctions / Screening	ROI through faster clearance, fewer false alerts
5%	Fraud Detection	Gains expected through anomaly detection, faster identification of fraud patterns

Barriers to adoption

Barriers to AI adoption continue to exist as organizations navigate three broad categories – people alignment, technical debt and the operational processes of being a compliance cost center and regulatory compliant. This signifies that innovations' success in compliance isn't primarily a technical challenge, but an organizational one.

People alignment

One of the strongest, most repeated themes by respondents is people alignment: senior leadership buy-in, cross-functional collaboration (Compliance–IT–Ops–Risk), and clear ownership/governance were cited repeatedly as key barriers to adoption. Close behind is capability building: training/upskilling, change-management, and growing a tech-oriented mindset across teams. Leveraging a partner setup was also seen as a viable approach to help, such as working closely with vendors/advisory partners, external guidance, and learning from peer institutions.

Technical debt

Legacy systems with limited integration options, data quality issues and budget constraints are rated by respondents as top barriers to AI adoption.

~20% Legacy systems with limited integration options

~20% Poor data quality or siloed setup

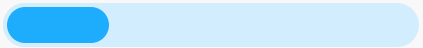
~21% Budget constraints and cost

Strategic considerations to address these include but are not limited to:

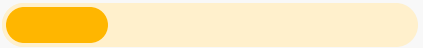
- ✓ Invest in modern platforms or consider middleware or API wrappers to connect legacy systems with AI tools. Do this in phases to minimize disruption and costs while enabling AI integration
- ✓ Establish a data governance framework to unify and cleanse data across departments, ensuring AI models receive accurate, consistent inputs for best results
- ✓ Prioritize cloud-based, scalable AI solutions with predictable costs and adopt modular approaches to spread investment over time rather than complete overhauls

Operational execution and performance

The **cost to innovate** alongside **good quality and available data and having the necessary skilled personnel** to support AI systems and AI governance, top the list by respondents. These were closely followed by 'regulatory uncertainty' as it relates to both AI regulations around the world and the expectations of regulatory bodies and supervisory teams overseeing financial institutions.



~23% Cost



~23% Data availability and quality

~21% Lack of skilled personnel

Strategic considerations to address these include but are not limited to:

- ✓ Assess cost (e.g., in-house vs buy) and implement AI projects incrementally to control spending and focus on areas delivering quick wins, demonstrating early ROI to secure further funding.
- ✓ Invest in ongoing data quality monitoring and build pipelines to ensure timely, comprehensive, and clean data feeds for AI systems.
- ✓ Implement strong data governance and cleansing to ensure consistent, accurate data that improves AI model performance.
- ✓ Invest in upskilling existing staff in AI essentials and leverage experts where possible, while adopting user-friendly AI tools that reduce dependence on specialized talent.

Human-in-the-loop oversight

Human-in-the-loop oversight is crucial in AI solutions to balance automation benefits with regulatory compliance, supervisory expectations, and governance standards. It ensures that AI-driven decisions are reviewed and validated by humans, preventing poor outcomes, biases, and unintended consequences in real-time and regulated environments.

This oversight also helps maintain accountability and builds trust with regulators and customers by providing transparency and control over AI processes. It enables organizations to leverage AI's speed and precision while retaining the critical judgment and expertise of human professionals.

The majority of respondents (69%) say human reviewers primarily focus on validating alert relevance, highlighting that AI-generated outputs still require a 'human-in-the-loop' to ensure accuracy and context.

63% cite making final case closure decisions, reflecting the regulatory and reputational risk associated with automating such determinations. Over half (**54%**) emphasize interpreting grey area outputs, suggesting that AI is valuable for volume handling and prioritization, but judgment-based decisions still rely on expert analysts. Meanwhile, **40%** involve humans in training or tuning models, showing a growing partnership between compliance teams and data science functions.

Only **32%** point to regulatory defensibility, indicating that while AI is assisting operational efficiency, formal regulatory justification frameworks are still developing.

As such, AI is augmenting, and humans remain vital to the process of providing judgment and oversight that technology cannot replace.

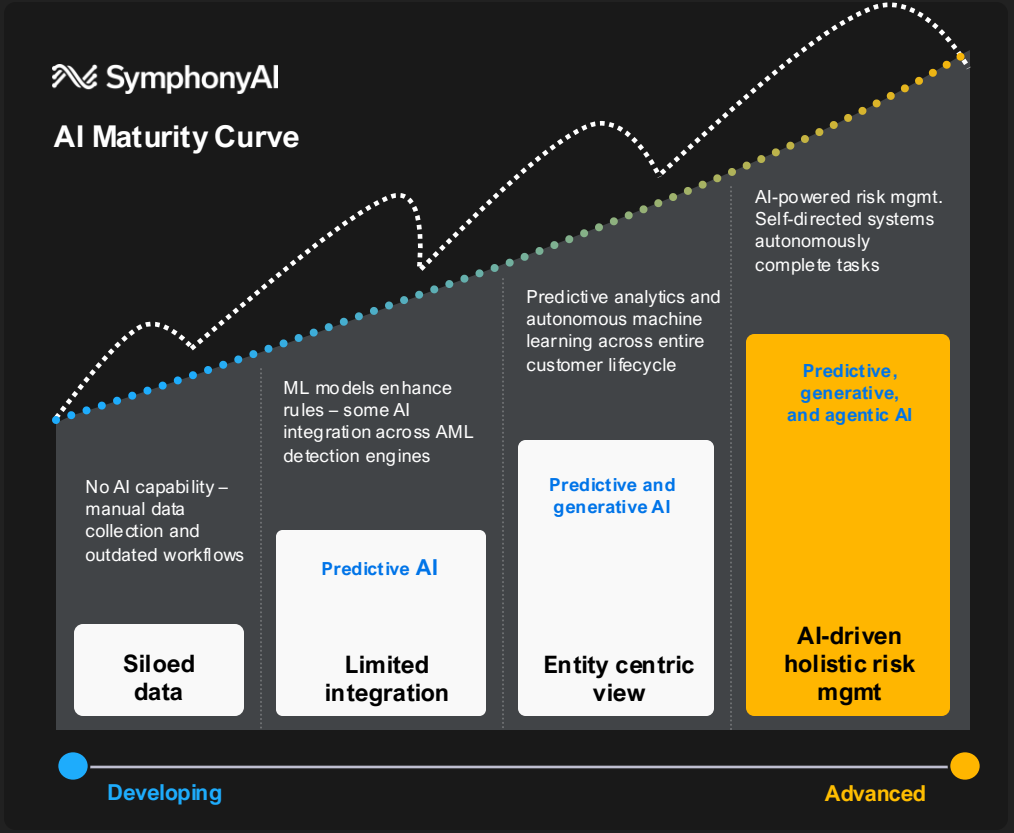
The close collaboration between humans and AI blends automation's speed with human insight to create smarter, more trusted compliance solutions.

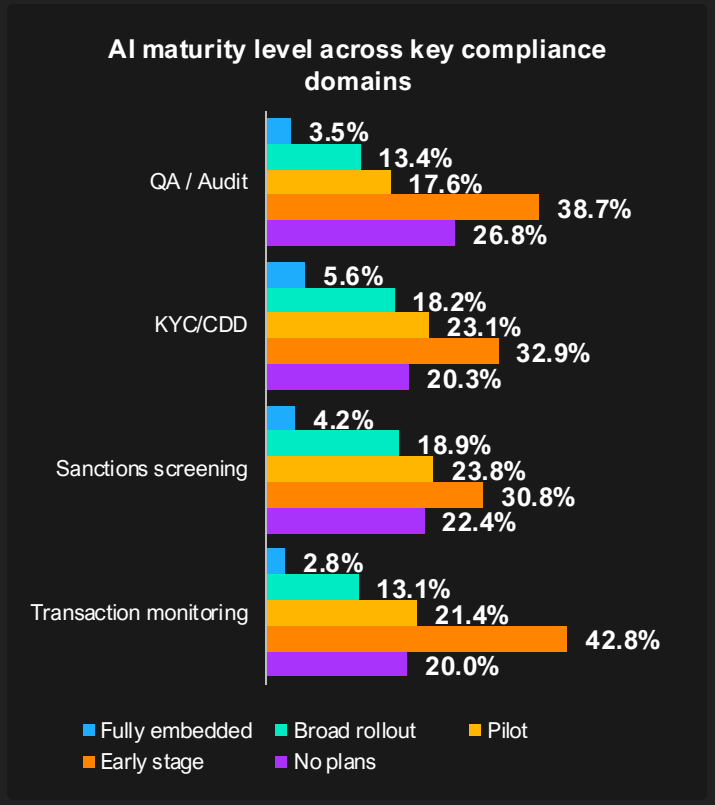
The AI journey - moving along the AI maturity curve

The AI maturity curve invites organization to pilot modest innovations confidently while keeping an eye on sweeping transformation. Success lies in balancing immediate results with scalable vision, evolving AI from isolated use cases into enterprise-wide intelligence.

Embracing a mindset of **continuous evolution** is key - beginning with quick-wins to build confidence and evidence value. This in turn, helps to maximize resources and technology while demonstrating ROI, and allowing value-driven and trusted automation.

According to the survey, the current stage of AI maturity across the financial crime domains shows strong ambition, with the majority of respondents being at **early stages (31–43%)** or **pilot phase (17–24%)**. Fewer than **6%** have AI fully embedded across any compliance domain.





The highest levels of AI maturity are visible in KYC/CDD (5.6% fully embedded) and sanctions screening (4.2%), both areas where structured data and process standardization make AI deployment more achievable.

Transaction monitoring shows significant experimentation, with **21%** piloting solutions, yet with relatively few at scale (13% broad rollout, 2.8% fully embedded).

Quality assurance/audit show similar results, reflecting the reliance on process analytics and human judgment, though it is gaining ground as organizations look to automate assurance functions.

AI maturity is also heavily influenced by **data quality, reliability and availability.**

Data readiness: The hidden engine behind AI power

The survey suggests that the confidence level in data readiness for AI is still generally low: only **33%** of respondents are mostly or very confident in their data, while **58%** admit to gaps, inconsistencies, or major challenges. Just **11%** feel very confident, with **9%** reporting no formal data governance in place.

This highlights a key issue. That AI and automation are only as effective as the quality and governance of the data behind them. Despite growing investment in AI tools and governance frameworks, data readiness remains a pain-point, with poor data quality and traceability posing compliance and audit risks.

These findings make clear that data maturity is fundamental to AI maturity.

To fully unlock AI's operational maturity and compliance benefits, organizations need to invest in data modernization – consolidating sources, improving lineage tracking, and automating quality control to counteract:

- **Siloed data to boost AI intelligence:** disconnected datasets and inconsistent semantics prevent models from learning complete patterns, making insights fragmented and unreliable.
- **Data governance to shape trustworthy AI:** without standardized data quality, lineage, and privacy controls, AI outputs risk bias, inaccuracy, and compliance breaches.
- **Mature data confidence to enable sustainable scaling:** unified, high-quality, and context-rich data allows AI systems to scale confidently across the AML and fraud lifecycle, sustaining long-term value and innovation.

Measuring what matters: the rise of AI-driven KPIs

In the coming 12-18 months, the difference between leaders and laggards will hinge not simply on who uses AI, but on who measures it best.

Leaders today should measure the success of technological innovations like AI in AML and fraud systems because it provides clear visibility into the real impact of these investments on operational efficiency, risk reduction, and regulatory compliance. Without measurable metrics, it is difficult to justify continued investment, when to mature further with AI use-cases, or identify areas where AI underperforms or requires adjustment.

Well-defined success indicators help ensure that AI tools deliver tangible benefits such as faster case resolution, fewer false positives, and improved detection accuracy, which ultimately protect the institution's reputation and financial stability.

Approximately **30%** of respondents stated they have no mature KPI framework for outcome driven innovations. Those which have, have opted for activity-based metrics to align with productivity, efficiency, or cost contributors. The top five reported KPIs:

False positive rate (27%) cited this as the top indicator of system efficiency and AI model precision. Tracking reductions on FP frees up investigators, allows genuine risk to surface quicker, and creates less regulatory fatigue.	• Targets efficiency gains • Emphasis shows that ROI is expected through efficiency first • Cost driver in AML/Transaction Monitoring
Case resolution time (~23%) focusing on investigation speed without losing accuracy and for improved alert closure efficiency.	• Targets efficiency gains • Reflects a desire for speed without losing accuracy • Shorter resolution times reduce backlogs, helps meet regulatory deadlines, and improves risk responsiveness
Detection accuracy (~18%), assessing precision in identifying genuine suspicious activity.	• Quality indicator • The next layer showing regulators and management that AI isn't just faster, but smarter
Automation gains (15%) linked to manual task reduction, reducing headcount, always-on near real-time processing through AI adoption.	• Targets efficiency / productivity / cost savings • Measures operational ROI in direct financial terms
Customer onboarding experience (9%), balancing fraud and AML prevention with customer experience efficiency.	• Reveals a forward-looking view - compliance isn't just about avoiding fines, but also about enabling smoother business growth

False-positive reduction

Assessing improvements in alert quality and investigative focus

Case resolution or investigation time

Tracking workflow speed and investigator productivity

Detection accuracy

Measuring precision and risk coverage across AML and sanctions models

Together, these metrics account for more than **90% of all KPIs** mentioned, highlighting the strong focus of financial institutions on efficiency, accuracy, and regulatory performance in AI-driven financial crime prevention. Notably, several respondents remain in early pilot stages and have yet to formalize enterprise-level KPIs, indicating that measurement discipline is emerging but not yet standardized across the industry.

Defining two or three KPIs around AI implementation is beneficial as it creates a focused framework for tracking performance without overwhelming teams with data. KPIs tailored to key challenges in financial crime, such as false positive rate reduction, time to decision, and detection accuracy, provide leaders with actionable insights to guide resource allocation and iterative improvements. However, it is crucial that KPIs are carefully selected to cover the dimensions of efficiency, accuracy, and compliance comprehensively; relying on too few or irrelevant KPIs risks overlooking critical outcomes or unintended consequences of AI deployment. Thoughtful KPI definition balances granularity with clarity, empowering departments to optimize AI's value in fighting financial crime effectively and sustainably.

AI-driven efficiency: measuring what matters

AI is now delivering measurable results across the compliance lifecycle. Yet, the pace and consistency of measurable value remains uneven across the sector.

Most respondents expect to achieve a **return on AI investments** within **12 to 24 months of implementation.** A smaller group reports faster payback of six to twelve months, typically among institutions with mature data foundations and established automation frameworks. Others anticipate longer horizons of up to three years, reflecting persistent challenges with integration, governance, and model confidence.

The two areas generating the most consistent ROI are:

- Transaction monitoring – where AI reduces false positives, accelerates triage, and automates lower-risk alert reviews.
- KYC/CDD – where machine learning enhances data accuracy, onboarding speed, and customer risk segmentation.

Smaller gains are also emerging in fraud detection, regulatory reporting, and staffing efficiency, as intelligent automation and risk-based prioritization streamline workflows and contain cost.

The range of ROI timelines highlights an uneven transformation. Success will depend as much on data quality and integration as on the algorithms themselves.

From experimentation to scaled intelligence

The survey findings reveal a clear pattern: efficiency gains emerge where strong data foundations, explainable automation, and measurable KPIs intersect. Yet progress remains uneven. Many organizations remain mid-journey on the maturity curve, navigating the tension between legacy constraints and emerging innovation.

> The next frontier will be shaped not by who adopts AI first, but by who operationalizes it most effectively, embedding automation, data integration, and human expertise into a cohesive, intelligence-led ecosystem.

The following **Efficiency Maturity Index** illustrates this evolution, contrasting the traits of reactive versus proactive compliance programs and mapping the industry's trajectory toward scalable, intelligence-driven efficiency.

Dimension	Reactive organizations	Proactive organizations
Detection model	Rule-based, retrospective	Predictive, continuous, adaptive
Automation level	< 50 % workflows automated	> 75 % workflows automated, > 50 % AI agent collaboration
Case management	Fragmented, manual triage, and long investigation timeframes	Centralized, AI-assisted triage and investigations to surface red-flags/data gathering/summary, adjudication
Data infrastructure	Siloed, inconsistent	Integrated, real-time
ROI measurement	Informal, anecdotal	Defined KPIs
Organizational mindset	Compliance as obligation	Compliance as strategic capability

Efficiency maturity index: reactive vs. proactive compliance
Source: SymphonyAI FinCrime Frontier 2025–26; benchmarking references: Deloitte, EY, and Accenture financial crime compliance studies (2023–2024)

True efficiency will only materialize when data modernization, automation, and AI governance converge. Institutions that achieve this integration will set the new standard for cost-effective, intelligence-led compliance across global financial services.

Strengthening AI model governance in FinCrime compliance

As AI becomes integral to financial crime detection, governance is no longer an abstract compliance concept – it is an operational discipline that ensures models are transparent, explainable, and accountable. While regulators have yet to prescribe detailed standards for AI model governance in AML, their message is clear – the technology used does not change the regulatory obligation. Institutions must demonstrate that AI enhances their ability to manage risk, detect crime, and meet compliance expectations.

This principle is reflected in the survey results: **governance has emerged as one of the defining challenges of AI adoption in financial crime.** While early adopters are formalizing policies and oversight mechanisms, a large portion of institutions remain in the development phase highlighting the opportunity for the sector to move from conceptual governance to structured, operational discipline.

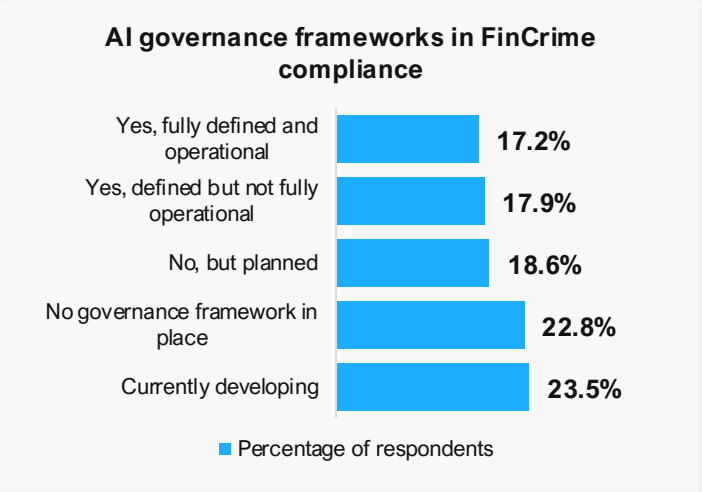
In financial crime compliance, AI governance is not just a generic practice. It requires deliberate evolution of policy and controls towards a risk-based approach, focusing on:

- Model ownership and accountability
- Data centricity and trust
- Auditability and explainability

Risk-based model governance

The data shows that governance maturity across the industry remains uneven. Only **17.2%** of institutions have a fully defined and operational AI governance framework, while another **17.9%** have frameworks in place but not yet fully operational. A further **23.5%** are still developing their frameworks, and **nearly one in four** organizations (22.8%) report having no governance structure at all.

This gap highlights the need for clear ownership, documented policies, and consistent oversight as AI becomes embedded in critical compliance processes such as transaction monitoring, screening, and customer due diligence (CDD). Without a formalized governance structure, institutions risk model drift, inconsistent decisioning, and potential regulatory exposure. For institutions scaling AI initiatives, the next frontier will be ensuring responsible, explainable, and auditable AI use, integrated with enterprise-wide risk management.



Model ownership and accountability

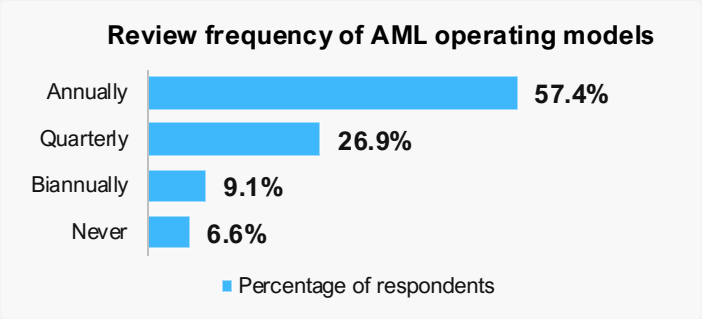
Governance begins with model ownership and accountability. Implementing AI in AML doesn't reinvent governance, it extends existing skillsets across key roles:

- **Model owners** must translate risk appetite and regulatory expectations into measurable AI performance indicators such as true/false positive rates, alert volumes, and detection efficiency. They must also know when to use AI versus rules-based methods balancing innovation with control.

- **Model developers** shift from purely rule configuration to data-driven optimization, using machine learning techniques alongside traditional logic. Their role now includes interpreting data signals, selecting appropriate algorithms, and maintaining documentation on model behavior (e.g., ROC AUC curves, feature importance, SHAP value plots).
- **Model users,** such as investigators and analysts, increasingly interact with AI-generated insights rather than static alerts. Their expertise is critical in validating AI outputs, recognizing nuanced patterns, and feeding high-quality feedback back into retraining processes, closing the loop in a continuous learning cycle.

These evolving roles illustrate that AI adoption in compliance isn't just a technical transformation – it is an organizational one. T**he most effective programs combine human judgment, explainable automation, and strong oversight.**

The survey reveals that **57.4%** of respondents review their AML operating models only annually, with another **26.9%** doing so quarterly. While annual reviews remain the norm, typically aligned with audit cycles and regulatory expectations – there's a growing cohort adopting more frequent reviews reflecting the need for agility amid evolving risks, regulatory updates, and technological advancements.



Institutions that perform regular, independent AML model reviews are better positioned to ensure effectiveness, maintain regulatory confidence, and adapt to emerging threats or changes in typologies.

Moving from annual validation to a risk-based, quarterly review cycle with continuous monitoring is a recommended action for a good model governance. Institutions that embed model health checks into everyday compliance operations will not only stay ahead of regulatory scrutiny but also improve detection quality and operational agility.

Data centricity and trust

AI models are only as strong as the data that fuels them. As discussed in the previous chapter, just over one-third of organizations express confidence in their data quality, while **58%** acknowledge known gaps, inconsistencies, or significant challenges.
Gaps in data quality and lineage undermine not only model performance but also explainability and auditability – two core expectations from regulators.

In this context, data governance has become the new compliance frontier. Organizations that modernize data infrastructure, strengthen lineage tracking, and automate data quality assurance will be better positioned to deploy AI responsibly and effectively.

Closing the data confidence gap

1. Establish a **single source of truth** by integrating fragmented data across AML, KYC, and sanctions systems.
2. Implement **automated data quality controls** and lineage tracking to detect inconsistencies in real time.
3. Assign **clear ownership,** with compliance and data teams jointly accountable for data integrity and regulatory defensibility.
4. Embed **continuous data audits and outlier detection** into AI models to ensure that decision making is centered around data familiarity.

Auditability and explainability: building trust in AI models

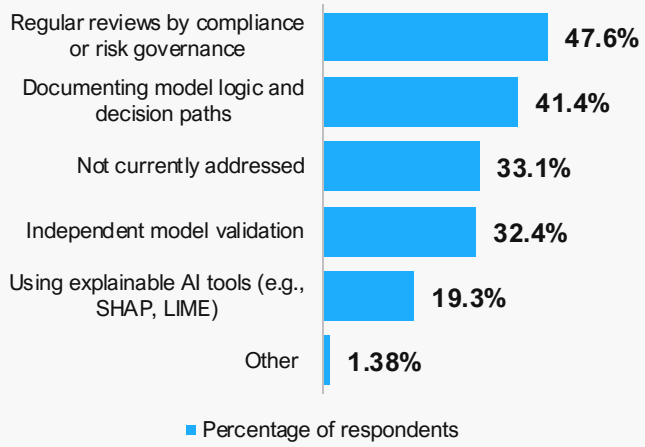
The results show that AI model explainability and oversight are still developing disciplines within compliance programs.

The most common practice, chosen by **47.6%**, is regular reviews by compliance or risk governance teams, suggesting that human oversight remains the cornerstone of explainability efforts.

41.4% document model logic and decision paths, aligning with regulatory expectations for auditability and transparency.

32.4% report independent model validation which reflects maturing governance processes, though fewer organizations have formalized frameworks compared to more traditional model risk management. Only **19.3%** report using dedicated explainable AI tools such as SHAP or LIME – indicating that while awareness of model transparency is rising, technical adoption of explainability frameworks remains limited. **A third (33.1%)** admit that explainability is "not currently addressed", underscoring that many organizations have yet to operationalize responsible AI practices in compliance contexts.

How firms ensure AI model explainability and compliance oversight



Multiple responses permitted; percentages may exceed 100%.

This signals that while traditional governance structures (e.g., reviews, documentation) are taking shape, technical explainability still lags behind operational oversight. As regulators increasingly emphasize transparency and traceability, organizations must move beyond manual reviews to adopt model-level interpretability tools and frameworks.

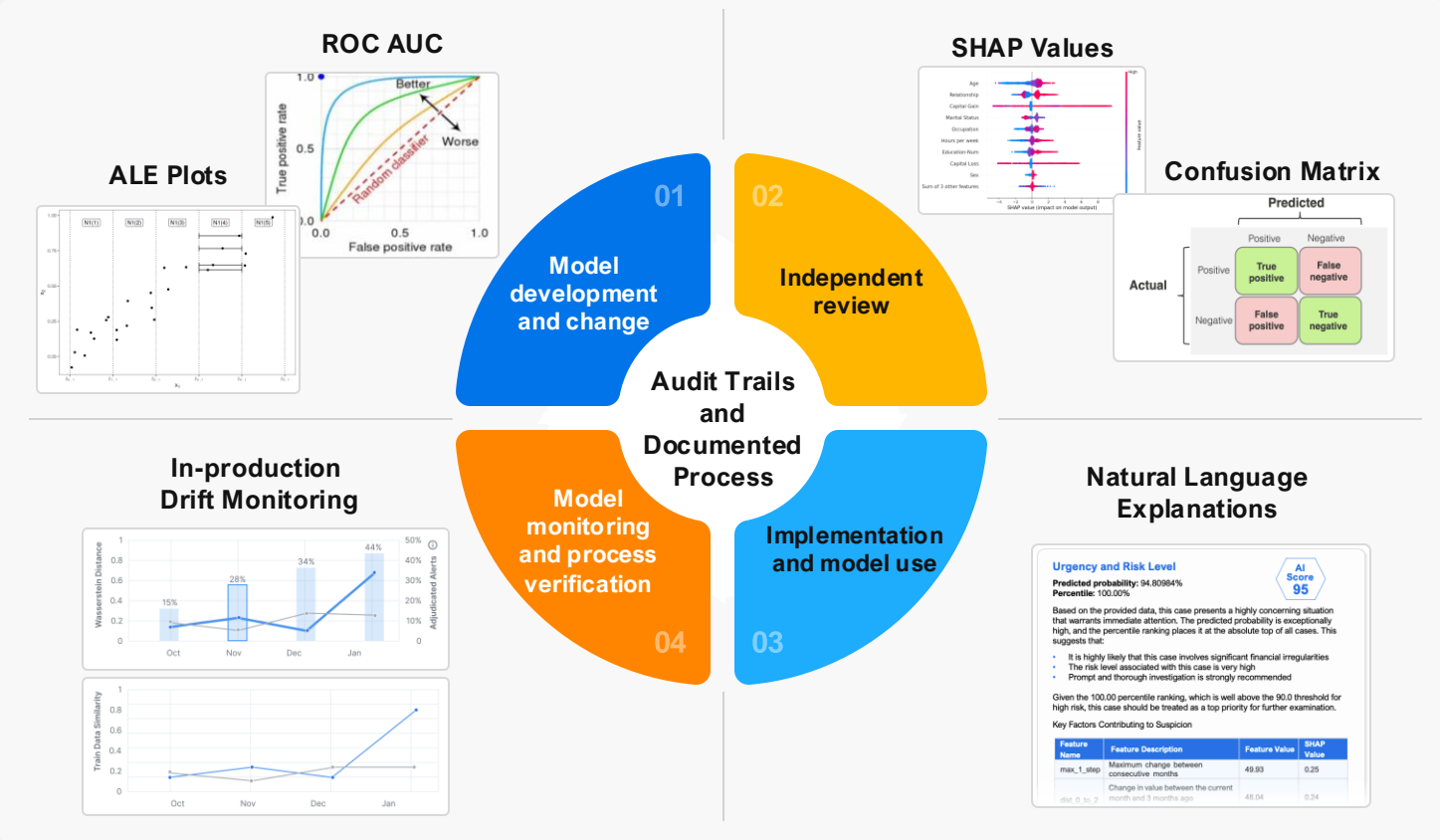
How to fast-track beyond manual reviews

Organizations can take **three pragmatic steps** to fast-track explainability maturity:

- **Integrate explainability into development:** standardize model documentation and logic capture from the outset. Automate generation of model documentation directly from development pipelines.
- **Adopt XAI tools and dashboards:** use frameworks like SHAP, LIME or ELI5 to visualize decision drivers and automate transparency. Leverage modern technologies such as explainability agents to increase clarity and transparency to end users and investigators.
- **Unify oversight:** connect compliance, data science, and audit teams through shared performance and explainability metrics. Establish a "human-in-the-loop" protocol that links policy, modelling, and investigation team.

What good AI governance looks like in FinCrime

AI model governance in financial crime builds on principles that institutions already know well from rule-based systems. In practice, the model lifecycle mirrors the familiar processes used in transaction monitoring or customer risk assessments – the difference lies in the additional complexity and rigor required to manage AI systems responsibly.



A mature governance framework typically includes:

- **Defined model ownership and roles** – delineating responsibilities across model owners (e.g., heads of transaction monitoring or screening), model developers (data scientists or analysts), and model users (financial crime investigators)
- **Independent review and validation** – often through a second- or third-line model risk function that assesses assumptions, methodologies, and data integrity before deployment
- **Continuous monitoring and drift detection** – tracking model performance, data changes, and alert quality over time to identify degradation or bias
- **Auditability and documentation** – maintaining traceable, pre-approved documentation that explains model logic, governance decisions, and sign-offs

This structured approach ensures AI-driven detection remains regulator-ready and resilient as underlying risks and datasets evolve.

Accountability and transparency: the cornerstones of responsible AI

Two principles dominate modern AI governance in compliance – accountability and transparency.

Accountability ensures there is always a clear "owner" of model behavior, decisions, and outcomes, even when algorithms drive detection logic. *Transparency* ensures that those decisions can be understood, validated, and explained to auditors, regulators, and internal stakeholders alike.

Leading institutions are incorporating:

- **Explainable AI** techniques such as SHAP or LIME to visualize model reasoning and feature weighting
- **Confusion matrices and performance dashboards** to track sensitivity and precision over time
- **Drift monitoring** to detect when underlying data or behavior changes make a model's assumptions invalid

Ultimately, governance maturity is about being able to answer a simple question: Can we explain and defend how our AI reached this decision?

Institutions that can do this will be able to demonstrate to regulators that AI is not a black box – it is a controlled, auditable system that strengthens compliance rather than weakens it.

From policy to practice: preparing for regulator expectations

While regulatory guidance on AI governance in AML is still evolving, the direction is unmistakable. Supervisors increasingly expect evidence of ongoing validation, model transparency, and documented oversight across the full AI lifecycle.

The most forward-looking organizations are already extending their enterprise-wide model risk management (MRM) frameworks to cover AI, applying consistent policies for model approval, testing, version control, and incident response.

AI governance is not separate from compliance governance. It is its next evolution. Organizations that embed governance and explainability into every layer of AI adoption will not only gain regulator confidence but also build more trustworthy, resilient, and effective financial crime detection programs.

Innovation and future outlook

The majority of respondents highlighted AI and machine learning (the dominant theme with ~70% of responses) as the most exciting trend in the fight against financial crime, particularly their potential to reduce false positives, enhance detection accuracy, and enable real-time, predictive monitoring.

It is therefore not surprising that the next two years will mark a decisive shift from AI exploration to strategic integration in compliance; nearly **80%** of organizations plan to implement AI in their AML and sanctions functions by 2026. **Transaction monitoring, name/PEP screening, and customer risk rating** emerge as the leading areas of implementation or pilot activity. This makes sense as they are the areas where large data volumes and repetitive processes make AI's impact most tangible.

Across all areas of financial crime compliance though, the majority of institutions remain in the early stages of AI adoption. Progress seemingly remains uneven due to data fragmentation, cost constraints, and skills shortages slow transformation.

Looking ahead then, the industry's evolution will be defined by three forces:

- **Trusted autonomy** – embedding explainable agentic AI to execute decisions safely.
- **Data collaboration** – federated learning and cross-institution intelligence sharing.
- **Human–technology synergy** – balancing automation with human-led judgment, accountability, and governance.

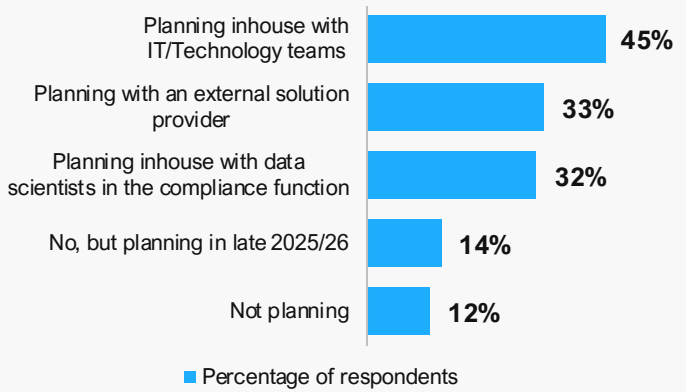
The AI adoption curve is steepening

Concerning institutional intent, the survey data confirms a turning point:

- **44.8%** plan to innovate in-house with IT or technology teams.
- **31.7%** will partner internally with compliance data scientists.
- **33.1%** will collaborate with external solution providers.

With nearly nine in ten organizations already preparing or progressing toward AI adoption, the compliance function is shifting from people- and process-centric to platform- and intelligence-centric where AI becomes the key structural enabler.

Plans to innovate with AI in the compliance function

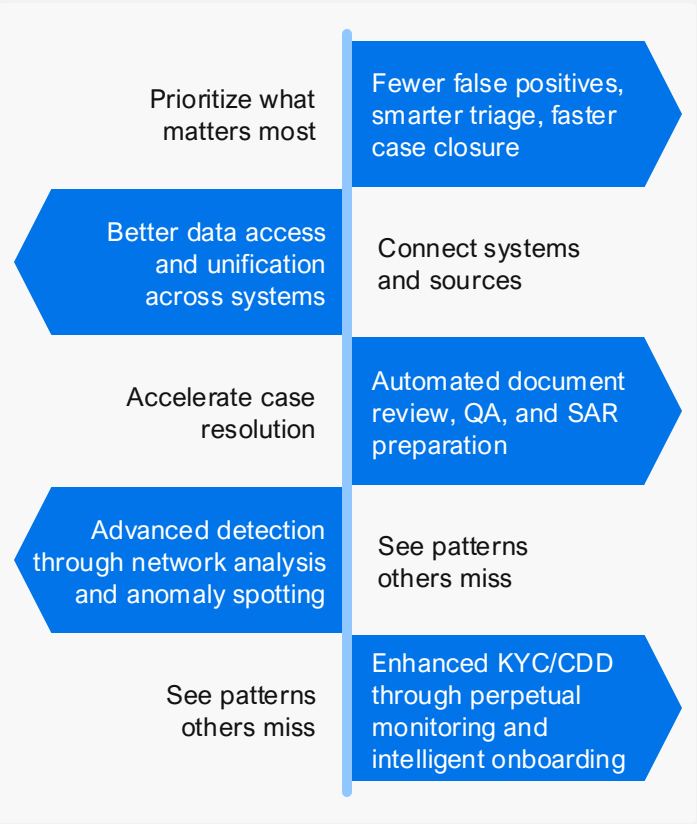


Multiple responses permitted; percentages may exceed 100%.

What compliance teams most want AI to fix

The market is demanding pragmatic AI. What this means in practice is that organizations require solutions that deliver measurable gains in precision, speed, and data accessibility.

Top desired AI outcomes:



Survey respondents highlighted their top priorities with AI focus on improving detection quality, data usability, and workflow efficiency to reduce manual effort, accelerate investigations, and strengthen overall compliance performance:

- **Alert volume and false positives:** The most dominant challenge by far is excessive false positives and alert volume, driving the need to reduce unnecessary transaction monitoring and sanctions alerts, improve alert relevance, accelerate disposition, and surface true positives earlier in the review process.
- **Data challenges:** Respondents highlight fragmented, inconsistent data as a major obstacle and call for unified, high-quality, lineage-tracked data with real-time access across sources to support faster, more holistic investigations.
- **Workflow automation and efficiency:** There is strong demand to automate repetitive investigative tasks (e.g., document reviews, case assembly, quality assurance, and reporting) in order to shorten case resolution times and, ideally, enable perpetual KYC monitoring.
- **Improved detection capabilities:** Institutions seek smarter, data-driven detection through anomaly and pattern recognition (including network and peer-group analysis, and fraud ring identification) to improve both true risk discovery and risk scoring accuracy.
- **KYC / CDD modernization:** Institutions aim to use AI to accelerate onboarding, enhance identity verification and adverse media screening, and automate analysis of financial documents such as bank statements.
- **Governance and model quality:** This includes model validation and scoring, regulatory defensibility, and continuous model training and tuning to maintain transparency and trust with regulators.

Don't expect wholesale change though, with **27.8%** respondents planning to spend their budget to **rip-and-replace their existing technology stack.** Intuitively, this makes sense, because ripping and replacing existing systems might not be a possibility for a variety of different reasons including long software contracts and budget constraints. As such, AI overlays are the answer for many institutions. Able to augment legacy systems with AI, they provide an efficient, scalable upgrade that boosts productivity, is cost-effective, and keeps pace with rapidly evolving technological demands without requiring a complete overhaul of existing infrastructure.

From AI experimentation to agentic AI revolution

The next phase of innovation will push beyond rule-based automation toward agentic AI, intelligent agents that work dynamically within predefined work scope and requirements. These AI agents can make decisions, plan, and learn from previous experiences. They can even collaborate with one another to seamlessly complete complex workflows.

Unlike AI copilots that support human investigators, autonomous AI agents take the lead in investigations, working together to analyze vast amounts of data, uncover hidden risks, and enhance decision-making. As with all AI used in financial crime prevention, human oversight is always present as a safeguard.

SymphonyAI's vision: an ecosystem where autonomous agents handle repeatable, rules-based compliance activities, allowing human experts to instead focus on areas where they work best - strategic oversight, model tuning, and investigative judgment in complex cases.

In effect, each investigation would run as follows:

- **Agents** triage, enrich, and resolve low-risk alerts autonomously.
- **Humans** provide strategic oversight and model supervision.
- **Systems** continuously learn from investigator feedback to optimize detection logic.

It is important to note that this evolution using agentic AI will not replace human expertise but amplify it, enabling compliance operations to evolve dynamically in real time.

Balancing innovation with regulatory confidence

As models grow more complex, regulators' focus on transparency, traceability, and accountability will intensify. The institutions that thrive will be those that integrate governance at the design stage, ensuring every decision made by AI can be explained, audited, and defended.

> As AI adoption deepens – from risk modeling to transaction monitoring – the question is no longer whether to innovate, but how fast and how safely; how strong an institution's AI governance is determines how safely it can innovate with the likes of agentic AI.

With this in mind, a **human-in-the-loop approach remains** essential. AI should augment and not replace human judgment, especially considering that the ethical or regulatory implications can be significant. By using expert oversight in automated processes, bias, model drift, and unintended outcomes can be counteracted before they affect critical decisions.

Alongside this, **explainable AI** is also imperative. Financial decisions cannot exist in a black box and must be transparent and defensible. Explainability builds confidence among regulators, clients, and internal teams by making AI-driven actions understandable and auditable.

Finally, **vendor due diligence and data quality** are central to controlling risk. After all, AI models are only as reliable as the data and third parties behind them. Poor data governance amplifies risks, meaning excellent data quality is the first safeguard in responsible AI deployment.

All of these points exemplify how SymphonyAI approaches financial crime compliance. Advanced explainable AI, human-in-the-loop throughout, and safe and secure guardrails to ensure that everything can be audited, defended and continuously improved.

The road ahead: collaboration and collective intelligence

The future of financial crime prevention is increasingly collaborative. Nearly half of industry experts express optimism about federated learning, the ability to share intelligence across institutions without sharing personally identifiable information (PII).

The idea is increasingly realistic given recent advances in technologies that preserve privacy, which now make it possible to navigate data transfer challenges across jurisdictions, enabling organizations to benefit from collective intelligence without breaching data protection rules.

However, for this approach to work at scale, several conditions must align:

- **Regulatory clarity and endorsement** on data handling and cross-border collaboration frameworks
- **Industry willingness** to participate, an idea grounded in trust and shared benefit
- **Strong governance** to ensure model transparency, fairness, and accountability
- **Technical readiness,** including standardized data formats and secure computation environments

If these elements come together, federated learning could mark a turning point in how financial institutions collaborate against financial crime. It will strengthen detection capabilities, improve typology awareness, and ultimately serve the greater good without compromising compliance or customer privacy.

A collaborative network of AI-driven compliance ecosystems that learn collectively to anticipate and disrupt financial crime faster than any single entity could manage alone is a truly exciting vision and one that SymphonyAI is actively working towards.

Outlook: the next frontier of compliance

The next frontier in financial crime prevention is likely to be using advanced technology such as **agent-based platforms and AI** to create a compliance infrastructure that adapts dynamically to regulatory changes and evolving threats. Today, we have reached a point where agents can fully automate critical processes such as alert triage, sanction screening, and transaction monitoring. However, forward-thinking companies are eager to push beyond these foundational capabilities. They are focusing on developing agents that enhance risk management, inform business decisions, and even serve as proactive workers in the field, turning compliance into a revenue-generating opportunity rather than simply being seen as a cost center.

This technological evolution will fundamentally reshape the landscape of financial crime, compliance, and risk management and even go further than that, outside of the currently defined ecosystem. By offering customers the ability to use these technologies for broader business enablement, innovation is no longer confined to a single use case. Instead, it becomes a continuous process, responding to the unique needs and ambitions of each organization. Importantly, these advancements will not impose limits but empower companies to imagine and implement new possibilities as their needs grow and change.

As institutions expand into new markets and jurisdictions, next-generation compliance technology relieves them from the burden of scaling traditional financial crime functions proportionally. The result? Unlocking their potential for significant growth, and the capacity to do business globally with confidence.

It is a hugely exciting time in the industry that is combining decades of expertise with state-of-the-art AI, creating systems that continuously learn and improve. Ultimately, this enables companies to fully automate their compliance functions from end to end, creating an adaptive solution that generates tangible value across the financial services sector.

Practical applications of agentic AI in FinCrime prevention

- **Fully automated alert triage:** Agentic AI can automatically review, classify, and handle alerts from sanction screening and transaction monitoring, reducing manual workload.
- **Dynamic rule and model updates:** Agents continuously track changes in regulatory environments and emerging threats, refreshing detection rules and models in real-time.
- **Risk management enhancement:** AI agents can analyze business data to improve and inform risk decisions and strategies.
- **Threat enrichment:** Agents collect and integrate new threat intelligence from customer data and adverse media, strengthening and updating fraud and financial crime detection capabilities.
- **Model governance and validation:** Agentic AI supports ongoing model validation, verification, and governance to meet regulatory standards and simplify risk management processes.
- **Business enablement:** Specialized agents can generate recommendations, uncover new business opportunities, and act as virtual field operatives, boosting revenue generation.
- **Jurisdictional compliance support:** AI agents help companies remain compliant as they expand into new regulatory territories and markets.
- **Customer-specific applications:** Solutions can be tailored to unique client needs, adapting agentic AI to specialized business and compliance requirements.
- **End-to-end compliance automation:** The ultimate vision is to automate the entire compliance process, from detection and alerting to investigation and reporting.

Alongside these agents, it's important to note that with current software, it is also possible for organizations to build their own agents to suit their specific needs.

While the technology and expertise needed to advance agentic AI in financial crime prevention are already available, the primary challenge lies in ensuring these solutions can be deployed within highly regulated environments while maintaining full compliance. Recent developments in Artificial General Intelligence (AGI) and self-learning, continuously adaptive agents offer promise in proactively identifying and mitigating new threats.

Historically, financial institutions have been reactive, often playing catch-up to increasingly sophisticated bad actors who rapidly adopt advanced technologies for phishing, scamming, and fraud. In fact, a leading concern among respondents is the growing sophistication of criminal tactics and tools (41.8%), underscoring how financial institutions view innovation in criminal networks as outpacing defensive technology and processes.

The next transformative leap then, is to reverse this way of thinking: self-learning AI systems can empower institutions to stay ahead of emerging risks, rather than simply responding to them. This forward-looking approach, which is possible today, enhances protection for both organizations and individuals, benefiting public trust and the safety of the global financial ecosystem.

Conclusion and strategic recommendations

The **FinCrime Frontier 2025-26** survey reveals an industry in transformation with AI usage no longer speculative, but a large part of improving compliance performance with **nearly nine in ten institutions** already implementing or planning to implement AI by 2026.

Looking deeper into the feedback, this is no surprise with compliance teams deploying intelligent automation to sharpen risk detection and reduce false positives, freeing up skilled analysts for higher value investigations. The most common adoption areas of transaction monitoring (39.3%) and screening (36.6%) highlight how AI is being used to strengthen both efficiency and decision quality.

Importantly, financial institutions are recognizing that the return on compliance investment extends beyond cost avoidance with AI delivering measurable value through faster alert resolution, improved detection accuracy, and enhanced audit readiness. These all directly affect other areas including business continuity, customer trust, and regulatory confidence. Even so, more should be done to highlight these improvements with only 28% of respondents having conducted a return on investment analysis for compliance technology investments despite people and technology accounting for roughly half of compliance spending.

People is the key word here; AI is not set to replace the world of work as we know it with 45% of institutions planning to enhance their existing systems with AI rather than replace them. This signals a shift towards incremental modernization that builds resilience and improvements without escalating costs.

Amid all this, governance maturity remains a differentiator. While 17.2% of organizations already have fully operational AI governance frameworks, many others are still developing theirs, which is a sign of cautious, active progress towards responsible, explainable AI use within financial services.

From the messages given within this report, bringing everything together effectively – technology, governance, people and training - can only be a good thing for the industry as it moves into this era of more effective and efficient compliance.

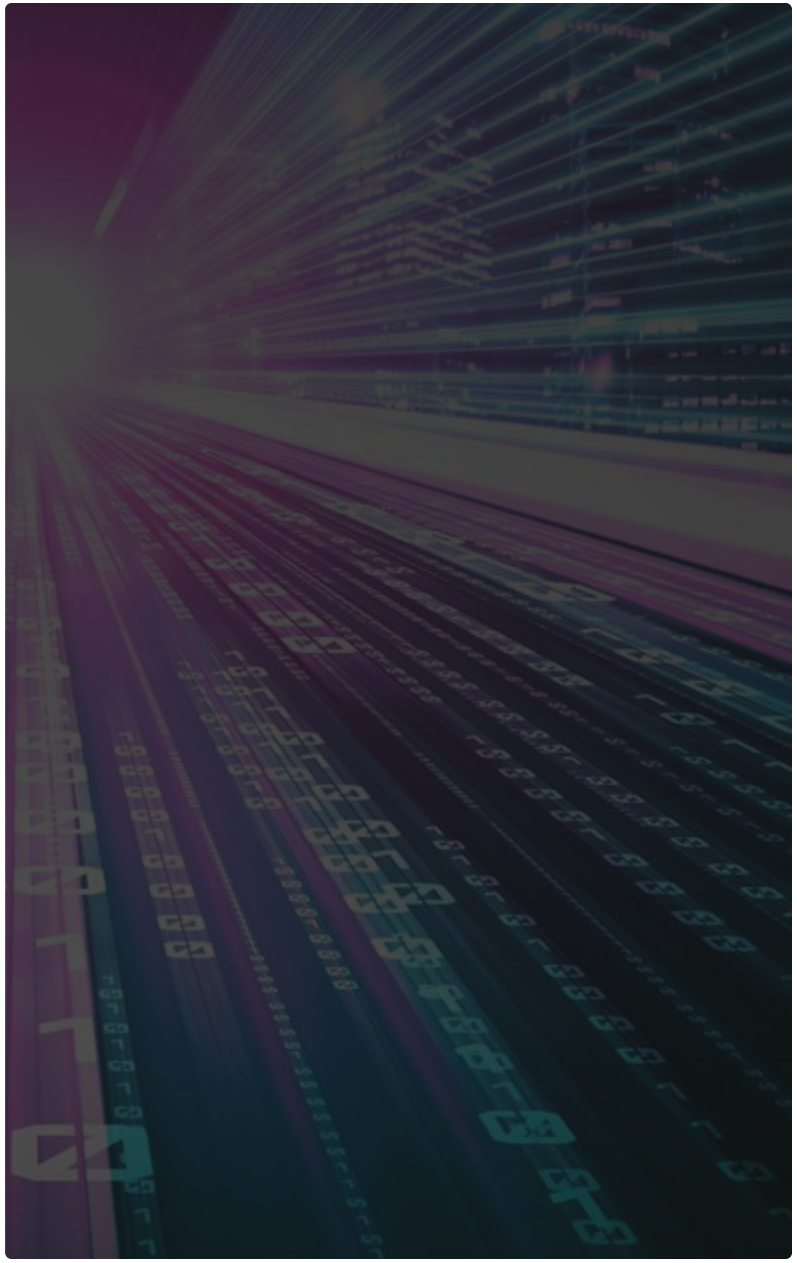
Key takeaways for compliance leaders

- **AI adoption is now mainstream.** With nearly 80% of respondents planning or implementing AI by 2026, the focus is shifting from proof of concept to measurable impact.
- **ROI transparency is lagging.** Almost three-quarters of institutions have never measured the return on compliance technology investment, creating risk of inefficient spending and missed optimization opportunities.
- **Governance frameworks are maturing unevenly.** Only 17% have fully defined AI governance, while 46% of respondents cited cost and data quality as barriers to scaling.
- **Data confidence is fragile.** Just 11% of institutions describe themselves as “very confident” in their data quality, with over half admitting to significant data issues or inconsistencies.
- **Regulatory sentiment is increasingly positive.** A majority (58%) see new regulations as enablers of modernization.

Strategic actions for compliance teams

To meet rising expectations while managing cost and complexity, compliance leaders should focus on six strategic imperatives:

1. **Institutionalize AI governance**
   Build formal oversight frameworks that clearly define model ownership, validation cycles, and documentation standards. This ensures that AI decisions are explainable, auditable, and regulator-ready.
2. **Integrate ROI measurement into compliance strategy**
   Treat compliance investment like everything else in a business by tracking KPIs including false positive reduction, investigation time saved, and improved detection accuracy to demonstrate tangible value. In this way, teams can quickly uncover the areas where more optimization is required.
3. **Elevate data quality**
   Standardizing data is a must to truly get the most out of AI. Alongside this, strengthen data governance through tracking data lineage, bias testing, and automated quality assurance to ensure reliable AI performance and defensible audit trails.
4. **Adopt incremental modernization**
   Follow the example of the 45% of institutions planning to augment existing tech stacks rather than replace them. By focusing on modular, scalable AI enhancements, efficiency gains can be delivered quickly.
5. **Use the 50/50 compliance model**
   The 50/50 compliance model balances AI automation with investigator expertise to maintain human oversight while getting the most out of technology.
6. **Engage regulators early and often**
   Build structured, transparent dialogue on AI use, governance, and risk management. Institutions that help shape evolving regulatory frameworks will be better positioned for long-term compliance success.



How SymphonyAI can support the journey

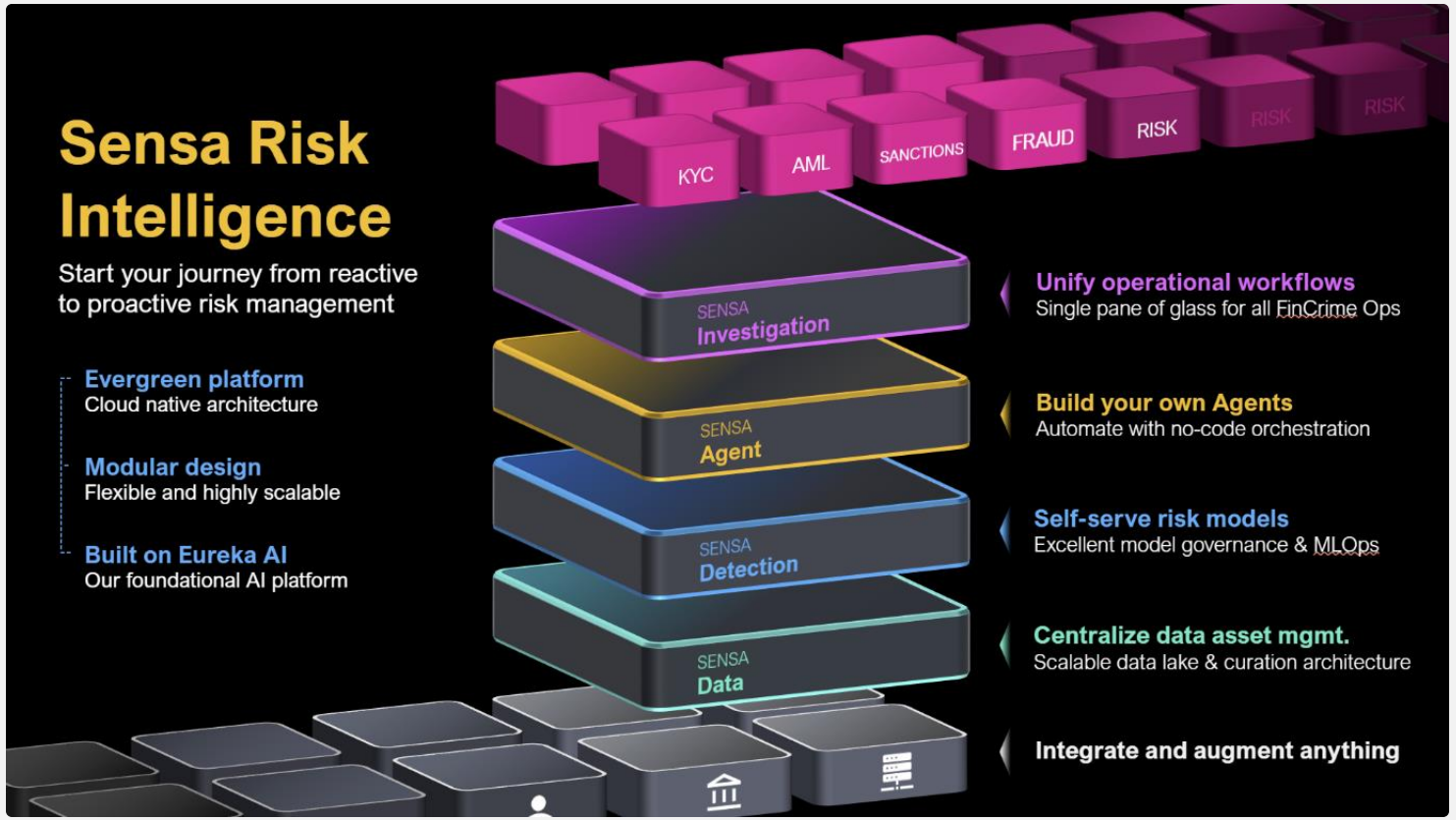
SymphonyAI's vision aligns directly with the technological transformation taking place in compliance.

Through **Sensa Risk Intelligence (SRI)**, SymphonyAI is helping institutions operationalize the very priorities surfaced in this survey - responsible AI adoption, transparent governance, and seamless data integration across compliance functions.

About Sensa Risk Intelligence

SRI is an AI-native FinCrime platform that's designed to help financial institutions move from reactive to proactive risk management. It centralizes and optimizes every aspect of compliance operations, from data ingestion and model management to investigation and reporting.

Every layer of the cloud-native platform has been built to leverage the latest predictive, generative, and agentic AI technology to enable greater automation, improved detection effectiveness, and significant operational efficiency savings.

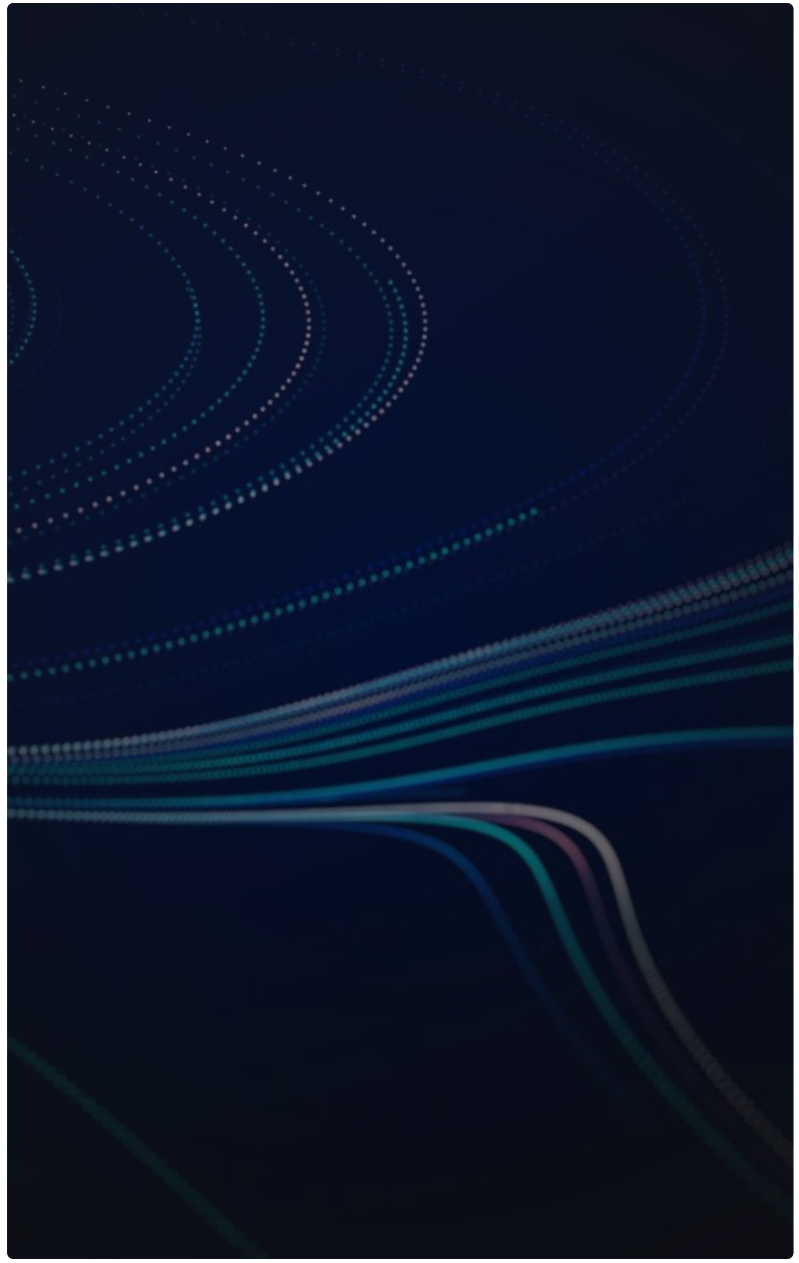


SRI comprises four modules:

- **Sensa Investigation:** Centralized, subject-centric case management that leverages AI agents to automate over 70% of manual tasks.
- **Sensa Agent:** An AI agent orchestration layer with 'build your own' agent functionality.
- **Sensa Detection:** Centralized rule and AI model management combined with AI-driven, no-code optimization capabilities.
- **Sensa Data:** Unify all data sources, apply AI-led entity resolution, and prepare your data to be AI-ready.

SRI represents a reimagining of the compliance operating model, built to eliminate legacy inefficiencies, unify fragmented systems, and turn compliance into a driver of business growth. It allows compliance teams to automate over 50% of the compliance workload with intelligent AI that transforms operational efficiency and reinvents the compliance function, turning risk mitigation into business acceleration.

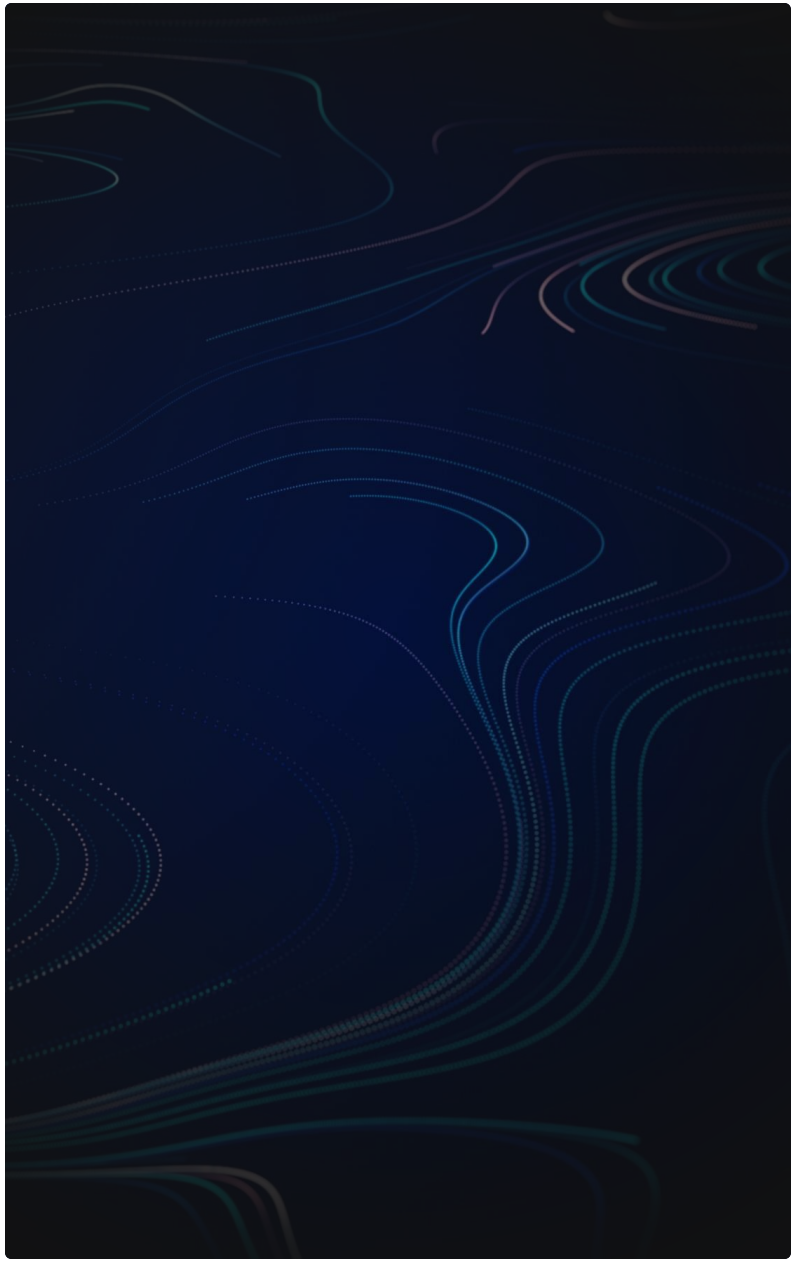
Visit Sensa Risk Intelligence for more information, or email us directly at connect.fs@symphonyai.com



Acknowledgment of contributors

The FinCrime Frontier 2025-26 report would not have been possible without the generous participation of the EMEA and Americas risk and compliance community. We extend our sincere thanks to all survey respondents for sharing their time, expertise, and insights, providing a vital, data-driven perspective on the state of financial crime prevention, AI adoption, and regulatory readiness worldwide.

We also wish to acknowledge the SymphonyAI Financial Services and AML Intelligence thought leadership teams for their collaboration in research design, analysis, and commentary. Their deep industry expertise and commitment to advancing innovation and integrity in financial crime compliance were instrumental in shaping this report.



SymphonyAI Financial Services

Jason Shane, Head of Product Strategy and Innovation
Charmian Simmons, Financial Crime and Compliance Expert
Elizabeth Callan, AML and Sanctions Expert
David Lehmani, Head of AI Incubation
Eric Murray, Product Director, Generative AI
Lala Huseynli, Marketing Lead, EMEA
Henry Fosdike, Content Manager
Chris Spratt, Product Marketing Manager

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 and Events Manager
Dervla McKenna, Marketing and Partnerships Executive
Alisson Bagnara, Tech Lead Software Engineer

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 Wadhwani, 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.

SymphonyAI

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.

AML Intelligence

www.amlintelligence.com