

advisense

An Advisense Insights Report | 2026

AML State of Play – Special Edition on AI

Foreword

Financial crime prevention is entering a decisive period. The EU Anti-Money Laundering Regulation (AMLR) is approaching, expectations on financial institutions are increasing, and AI continues to develop at remarkable speed. Together, these forces are changing not only how organisations comply, but how we should think about the future of financial crime prevention.

At Advisense, this is one of the reasons we continue to conduct our AML State of Play survey. Since 2022, our ambition has been to follow how the industry is responding to change and to contribute new perspectives to the discussion. By bringing together the experiences of financial institutions with what we see across the market, we hope to challenge established thinking and provide a useful basis for the decisions ahead.

Our 2026 findings show that the conversation has clearly moved forward. Awareness of the AMLR has increased significantly, implementation is becoming more tangible, and AI is moving from discussion towards practical use. At the same time, progress brings a different set of questions. The challenge is increasingly less about understanding what is coming and more about whether organisations have the governance, data, technology and organisational capacity to deliver it.

For me, this is the most important message from this year's survey. AMLR should not be approached simply as another regulatory implementation exercise, and AI should not be treated as a separate technology initiative. Instead, AML leaders, management teams and boards should ask a more strategic question: what do we want our financial crime prevention capabilities to look like in the years ahead? Which parts of today's framework should be strengthened, reconsidered or supported by technology and AI?

I am encouraged by the direction reflected in this year's findings. The industry is moving forward, experience is growing and the potential of new technology is becoming more tangible. But the next step requires deliberate choices. Organisations that understand where they stand today, set a clear direction and bring together the right people, technology and governance will be better positioned not only to meet the requirements of 2027, but to build stronger financial crime prevention capabilities for the future.

I hope this report contributes to that discussion and helps leaders make these choices with greater confidence.



Executive Summary

A fundamental change in the European anti-money laundering framework is drawing closer. From July 2027, the EU Anti-Money Laundering Regulation (AMLR) will introduce a directly applicable single rulebook, requiring financial institutions to reassess governance, customer due diligence, data management, monitoring, reporting and the technology supporting these processes.

Since 2022, Advisense has conducted a series of AML State of Play surveys to assess the evolving state of anti-money laundering (AML) and counter-terrorist financing (CTF) across the financial sector. The initiative provides a recurring perspective on industry maturity, progress and the challenges facing financial institutions as they strengthen their AML/CTF frameworks.

The 2025 report captured a market that recognised the scale of the AMLR transition but remained uncertain about what implementation would require in practice. Our 2026 findings suggest that awareness of the AMLR is materially higher, cross-functional implementation structures are taking shape, and organisations have a clearer view of the role technology may play. At the same time, AI is moving from exploration towards identifiable applications and day-to-day use.

The results indicate that awareness is no longer the principal issue for most respondents. Instead, attention is increasingly moving towards the operational consequences of the AMLR: how much data must be collected and reported, how governance structures need to change, which systems can support the requirements, and how different functions across an organisation will need to work together.

Key Findings

- AMLR implementation is accelerating. 67% of respondents describe their organisation as very aware of the AMLR and actively implementing it, compared with 14% in 2025.
- The operational impact will be broad. Group-wide compliance governance and customer data management/KYC remediation are jointly identified as the areas expected to have the greatest operational impact, each selected by 67%.
- Implementation is increasingly cross-functional. 56% report an extensive approach involving functions such as Compliance, Legal, IT and Data.
- AMLR is reinforcing technology investment. 67% expect the regulation to increase or significantly accelerate technology adoption, while 33% expect relatively little change to existing technology plans.
- AI is emerging in specific AMLR use cases. Risk assessment and customer risk scoring is the most frequently identified area where AI could support compliance, selected by 78%, followed by enhanced due diligence and transaction monitoring/suspicious activity detection, both at 56%.
- Technology concerns are shifting towards execution. 67% identify uncertainty over which technology will meet AMLR requirements and 67% highlight the implementation timeline, while 56% cite cost and the ability to demonstrate return on investment.
- Data is a defining implementation challenge. All respondents identify managing increased data-reporting obligations as one of the AMLR requirements they expect to be most challenging.

This is consistent with the broader transformation perspective. As understanding matures, AMLR readiness increasingly becomes a question of whether institutions possess the underlying capabilities required to translate regulatory requirements into sustainable operations.

The 2026 survey points towards a particularly important implementation dimension: data. Customer data management and KYC remediation is among the most frequently identified operational impacts. Increased data-reporting requirements are overwhelmingly regarded as a compliance challenge. Data quality and availability also remain one of the principal obstacles to implementing AI within AML/CTF. Linked to this, the issue of dealing with legacy systems remains.

Seen from this perspective, AMLR can become a catalyst for a more data-driven and technologically enabled approach to financial crime prevention. Success will depend on an organisation's ability to bring regulation, data, systems, governance and people together within a coherent transformation programme.

The strategic objective should therefore extend beyond achieving compliance by July 2027. The investments being made today should also contribute to a financial crime prevention framework capable of responding to evolving risks, regulatory expectations and technological opportunities in the years ahead.

Overall, this suggests that the central question is shifting from whether institutions understand the significance of AMLR to whether they can execute the required transformation in time.

AI forms one part of that transformation, but the findings point towards a pragmatic rather than technology-led approach. Organisations are primarily introducing AI around established processes and maintaining substantial human oversight. The immediate opportunity may therefore lie not in replacing existing AML controls with AI, but in determining where AI and automation can strengthen data processing, analysis, monitoring and decision support within a controlled operating model.

It also puts a critical strategic choice in front of AML leaders: which capabilities are the low-hanging fruit that can simply be brought into compliance with AMLR, and which should be fundamentally reimagined to build a more effective, future-ready financial crime framework?

Background of This Report and the Respondents

With this report, Advisense aims to provide an updated view of how financial institutions are preparing for the forthcoming AMLR requirements, what areas they expect to have the greatest operational impact, and what implementation challenges are becoming most prominent as the July 2027 application date approaches.

The 2026 edition of Advisense AML State of Play Report for Sweden explores the relationship between AMLR implementation and technological change. This reflects a central premise of Advisense 2025 edition in this series: the AMLR is expected to increase requirements for data governance, data management and analytical capacity, creating stronger incentives to reconsider how technology and AI can support financial crime prevention. The 2025 report was explicitly designed around this relationship between AMLR readiness and AI adoption.

The 2026 survey included 19 respondents from a diverse range of financial-sector organisations, including banks, lending and credit institutions, payment service providers, crypto and digital asset service providers, and life insurance companies. While the number of respondents was somewhat lower than in 2025, the survey still provides a meaningful indication of the priorities, challenges and developments shaping the sector.

These requirements remain the foundation for the 2026 analysis. However, the latest survey provides an opportunity to assess how organisations' perceptions have developed as implementation planning progresses.

The Respondents

Large organisations account for 68% of the 2026 respondents, compared with 36% in the 2025 survey. The professional backgrounds of respondents are also broader than in the previous study, although Compliance and AML remain the largest category: Compliance/AML Officer 53%, Specially Appointed Executive ('Särskilt Utsedd Befattningshavare')/First line 21%, Risk Management 11%, C-Suite Executive 5%, Business Development 5%, Other 5%.

Distribution of respondents across financial institutions



This is consistent with the broader transformation perspective. As understanding matures, AMLR readiness increasingly becomes a question of whether institutions possess the underlying capabilities required to translate regulatory requirements into sustainable operations.

The 2026 survey points towards a particularly important implementation dimension: data. Customer data management and KYC remediation is among the most frequently identified operational impacts. Increased data-reporting requirements are overwhelmingly regarded as a compliance challenge. Data quality and availability also remain one of the principal obstacles to implementing AI within AML/CTF. Linked to this, the issue of dealing with legacy systems remains.

Seen from this perspective, AMLR can become a catalyst for a more data-driven and technologically enabled approach to financial crime prevention. Success will depend on an organisation's ability to bring regulation, data, systems, governance and people together within a coherent transformation programme.

The strategic objective should therefore extend beyond achieving compliance by July 2027. The investments being made today should also contribute to a financial crime prevention framework capable of responding to evolving risks, regulatory expectations and technological opportunities in the years ahead.

Overall, this suggests that the central question is shifting from whether institutions understand the significance of AMLR to whether they can execute the required transformation in time.

AI forms one part of that transformation, but the findings point towards a pragmatic rather than technology-led approach. Organisations are primarily introducing AI around established processes and maintaining substantial human oversight. The immediate opportunity may therefore lie not in replacing existing AML controls with AI, but in determining where AI and automation can strengthen data processing, analysis, monitoring and decision support within a controlled operating model.

It also puts a critical strategic choice in front of AML leaders: which capabilities are the low-hanging fruit that can simply be brought into compliance with AMLR, and which should be fundamentally reimagined to build a more effective, future-ready financial crime framework?

In this year's edition of the survey, the analysis is extended with additional questions concerning actual AI use, human oversight, current tool types, operational impact, future expectations and regulatory concerns. Hence the report distinguishes between direct year-on-year comparisons and broader directional comparisons.

The results are intended to provide a directional indication of current practices, how priorities and implementation challenges are evolving, rather than statistically representative changes across the wider financial sector. As such we hope to contribute to the broader discussion and provide this report to serve as a basis for discussion around the AMLR and the evolving use of AI within AML/CTF.

Delimitation

The findings presented in this report are based on responses from a limited number of participating organisations and should therefore be interpreted as indicative of current market perspectives rather than statistically representative of the financial sector as a whole. Response rates also vary between individual questions, and percentages should be considered together with the underlying number of responses.

The report is structured around principal issue areas covering the current awareness of the AMLR, perspective on operational impact, compliance challenges, cross-functional coordination, potential AI applications, expectations around technology investment and technology/AI strategy.

The survey poses around twenty questions around core issues including:

- Awareness of the forthcoming EU Anti-Money Laundering Regulation requirements.
- Areas where the AMLR is expected to have the greatest operational impact.
- Areas within the AMLR that organisations anticipate will be most challenging to comply with.
- How organisations manage AMLR implementation involving functions such as Compliance, Legal, IT and Data.
- How AMLR will impact the approach to using technology in compliance.
- Aspects of AMLR compliance where AI could most help organisation address.
- Key concern about AMLR implementation in relation to technology/AI strategy.

Setting the Scene: From Regulatory Implementation to Transformation

The EU AML Package creates a common framework for combating money laundering and terrorist financing, with the AMLR single rulebook introducing directly applicable requirements across the EU. The AMLR will substantially strengthen requirements for governance, CDD, data management and monitoring, while the EU-level authority AMLA aims to promote more consistent supervision and enforcement.

With the 10 July 2027 implementation date drawing closer, organisations should look beyond compliance and view AMLR implementation as an opportunity for broader transformation.

Implementation as a conventional compliance exercise, performing an article-by-article gap analysis to identify additional requirements, update policies and processes, and add another layer of controls to existing infrastructure risk not achieving the necessary results. This approach is a recipe for reproducing the same structural weaknesses by layering new obligations onto architecture that was not designed to support an effective and risk-based financial crime prevention framework.

Rather than asking only what must change to comply with the new regulation, financial institutions can use the implementation programme to reassess how their financial crime prevention framework should operate in the future

This is particularly important considering that AMLA has signalled a supervisory direction that is increasingly data-driven and evidence-based rather than primarily document-driven. Institutions will therefore need not only to demonstrate that policies and frameworks exist, but increasingly provide evidence through data that their risk-based approach works in practice. This has several important consequences.

First, the AMLR is as much a data and infrastructure challenge as a regulatory one. Requirements concerning beneficial ownership verification, customer risk classification, transaction monitoring, audit trails, information sharing and responses to authorities ultimately depend on the ability to access, connect, process and retrieve reliable data. These requirements therefore extend beyond policies and place direct demands on systems, data architecture and performance across the organisation.

Second, the AMLR reinforces the move towards compliance as a continuous state rather than a periodic exercise. Dynamic CDD, ongoing transaction monitoring and real-time screening sit uneasily with operating models designed around fragmented manual processes, periodic controls and annual reviews. The implementation challenge consequently extends into process design and the underlying operating model.

Third, the risk-based approach itself will increasingly need to be demonstrable and evidence-based. The organisation will need data, analytics and auditability capable of demonstrating how risk assessments translate into actual controls and decisions.

AMLR implementation reaches well beyond the Compliance function. It is simultaneously a governance, process, data, analytics, technology and organisational capability programme, which is why AI inevitably will play a key role.

1. Expected Operational Impact of AMLR

Q1 "How would you rate your organisation's awareness of the forthcoming EU Anti-Money Laundering Regulation requirements?"

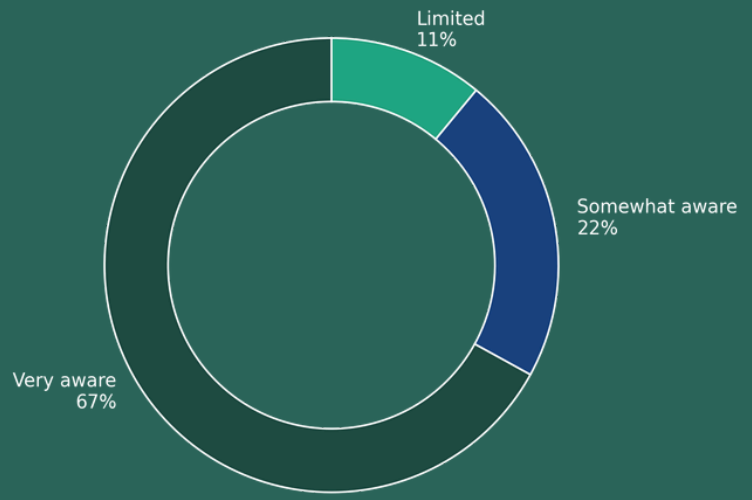
The finding should be interpreted with the differing respondent bases in mind, but the direction is clear: awareness has matured considerably as the implementation deadline approaches.

Whereas the 2025 results portrayed a market in which most organisations knew about the AMLR but had not yet developed a detailed understanding, the 2026 responses indicate that active preparation is now the dominant position among respondents.

In 2025, only 14% of respondents described their organisation as very aware of the AMLR. The majority, 64%, reported being somewhat aware, while 21% indicated limited awareness.

AMLR Awareness in 2026

Figure 1: Awareness of the forthcoming AMLR requirements, 2026



In 2026, 67% describe themselves as very aware and actively preparing, 22% report a general understanding, 11% report limited awareness – and no respondents are unaware of the AMLR.

The finding also highlights a broader challenge in the transition from AI experimentation to more mature adoption. Organisations need regulatory compliance expertise to develop alongside technological capability. This means bringing together compliance, legal, risk and technology expertise to understand which requirements apply, how they interact and what this means for the design, governance and oversight of AI-supported processes – which can be translated into knowledge to identify and navigate potential areas of tension in the first place.

Q2 "Which AMLR areas do you expect will have the greatest operational impact on your organisation?"

Understanding the AMLR at a conceptual level is different from grasping what it will mean for day-to-day operations. In 2025, 67% identified group-wide compliance governance and structure as their number-one expected area of impact. Customer data management and KYC remediation also featured strongly, while beneficial ownership transparency was another noteworthy area.

In 2026, respondents were asked to select up to two areas where the AMLR is expected to have the greatest impact.

Figure 2: AMLR areas expected to have the greatest operational impact



What appears to have strengthened in 2026 is the importance attached to customer data management and KYC remediation, which now stands alongside governance as the most frequently selected operational impact.

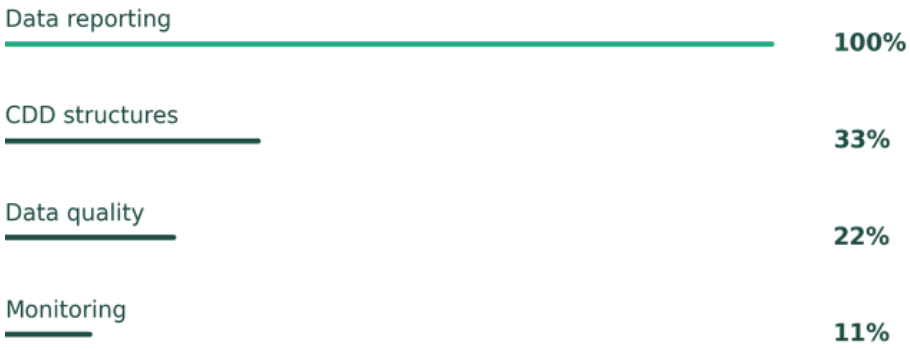
This is an important development. It indicates that financial institutes increasingly see AMLR implementation as not only an organisatioal and governance exercise, but also as a major data-management programme.

Q3 "Which AMLR areas do you anticipate will be most challenging to comply with?"

The perceived compliance challenges show a more pronounced change. In 2025, respondents ranked ongoing monitoring as the leading compliance challenge, followed by ensuring data quality and audit traceability. Increased reporting obligations ranked third, followed by establishing group-wide policies across jurisdictions.

In 2026, respondents were asked to select up to two challenges.

Figure 3: AMLR areas anticipated to be most challenging to comply with



> Every respondent answering the 2026 question selected increased data-reporting obligations as one of their two most significant expected compliance challenges.

What can be observed is a clear shift in emphasis towards the scale of data reporting required under the new framework. Every respondent answering the 2026 question selected increased data-reporting obligations as one of their two most significant expected compliance challenges.

This may not necessarily mean that ongoing monitoring or data quality have become less difficult. Rather, the results suggest that as organisations develop a more practical understanding of the AMLR, the volume, structure, traceability and operational burden of data becomes increasingly visible.

The result is also consistent with the broader view of AMLR as an opportunity for data-infrastructure transformation. If supervisory expectations increasingly require institutions to demonstrate the effectiveness of their risk-based approach through data, reporting capacity and traceability are likely to become central implementation capabilities.

Q4 "To what extent does your organisation have an AMLR implementation plan which includes cross-functional coordination involving functions such as Compliance, Legal, IT and Data?"

One of the clearest messages from the 2025 report was that AMLR implementation could not be managed exclusively within Compliance. The 2026 findings provide a useful indication of implementation maturity.

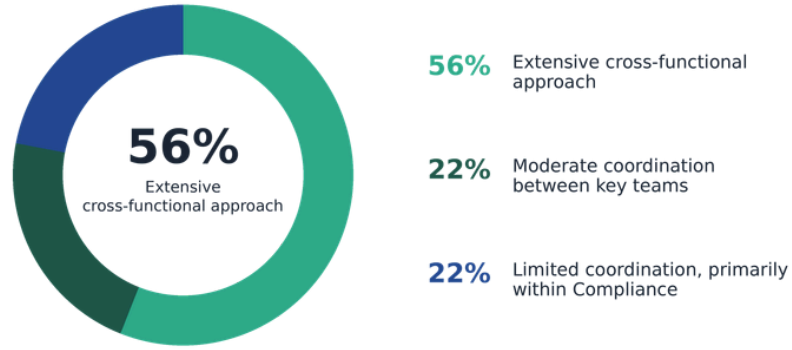
AMLR implementation touches business functions, technology, compliance, data and operations simultaneously, this matters from a transformation perspective. Cross-functional coordination therefore needs not only participation, but sufficient mandate to resolve dependencies and make decisions across organisational boundaries.

> More than half of respondents report that their AMLR plans already involve a broad combination of Compliance, Legal, IT and Data.

More than half of respondents report that their AMLR plans already involve a broad combination of Compliance, Legal, IT and Data. This is a slight increase from 2025, when 50% of respondents expected extensive enterprise-wide coordination and 50% expected moderate coordination between key teams.

Regarding the extent to which the respondents organisation's actual AMLR implementation plan already includes cross-functional coordination:

Figure 4: Cross-functional coordination in AMLR implementation plans



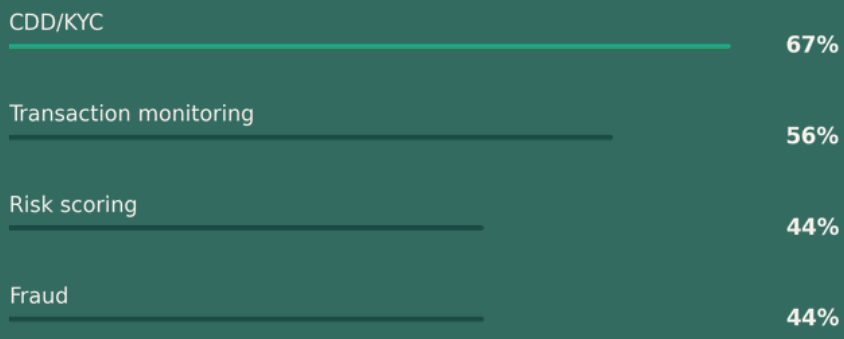
2. Current Use of AI in AML/CTF

The following survey questions explore where organisations are applying or considering AI, how they prioritise use cases, what is driving adoption, how AI is being integrated into existing processes, and the key barriers to implementation.
Taken together, the findings suggest a pragmatic approach to AI adoption. Organisations are initially focusing on established financial crime processes where operational challenges are well understood and the potential benefits of AI are more tangible.

Q5 "Where is your organisation currently applying or considering AI within AML/CTF?"

The results indicate that organisations see opportunities for AI across several parts of the AML/CTF lifecycle rather than in a single specialised application. Particularly notable is the prominence of CDD/KYC, transaction monitoring and customer risk scoring.

Figure 5: Where AI is currently applied or considered within AML/CTF



This represents a logical progression, given that these activities involve significant and increasing volumes of customer, transactional and contextual information and require information to be collected, assessed and updated across different systems and sources.

The result should not, however, be interpreted as evidence that AI is already operational across all of these areas. The question covers both applications currently in use and those under consideration. It is therefore better understood as an indication of where organisations currently see the most immediate potential for AI.

Q6 "What is the rationale for selecting these areas for AI application as the most immediate opportunity?"

The responses indicate a strong preference for use cases capable of producing relatively immediate value. 89% of respondents identify applications that can add value quickly with relatively low effort as the rationale for their choice. The remaining 11% identify low risk as the principal rationale.

This provides an important indication of how organisations are prioritising AI use cases. Rather than beginning with the most technologically ambitious applications, organisations appear to favour areas where the problem is already understood and where AI can potentially be introduced without fundamentally redesigning the underlying process.

AI investments compete with regulatory implementation, business-as-usual activities and other technology priorities. The ability to demonstrate tangible value relatively quickly may therefore be important when determining which use cases progress from experimentation to implementation.

Such an approach is consistent with an incremental implementation model. Initial AI adoption is likely to be easier where organisations already understand the workflow, available data and operational bottleneck they are attempting to address. It may also reflect the practical circumstances facing Compliance and AML functions

Q7 "What are your organisation's primary motivations for implementing AI in AML/CTF?"

Respondents were asked to rank five motivations, with a ranking of one representing the primary motivation. The overall order was:

1 Operational efficiency / cost reduction
2 Reducing false positives
3 Improving detection rates
4 Competitive advantage
5 Regulatory compliance

Organisations are particularly interested in whether AI can make existing AML/CTF processes more efficient, reduce unnecessary manual work and help focus resources on activities that warrant greater attention.

Operational efficiency and cost reduction was identified by 44% as their primary motivation, followed by reducing false positives ranked first by 33%. Improving detection rates and regulatory compliance each received first-place ranking by appr. 10%, while no respondent ranked competitive advantage as their number one motivation.

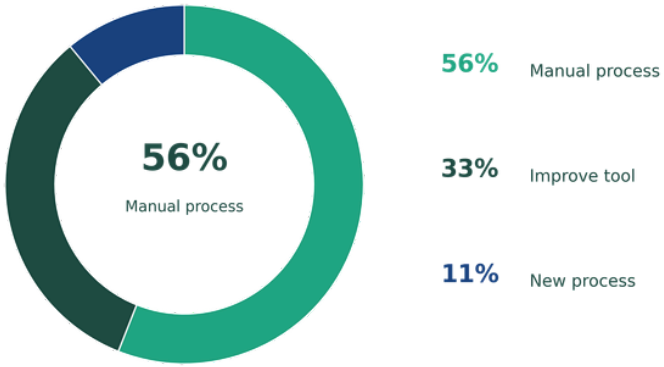
Regulatory compliance ranks comparatively lower as a direct motivation. This should not necessarily be interpreted as indicating that compliance considerations are unimportant. Rather, the findings suggest that organisations increasingly expect AI investments to generate operational value alongside supporting compliance objectives.

The prominence of reducing false positives and improving detection rates reinforces this picture. Both address a longstanding challenge of having to process large volumes of information and alerts while directing human expertise towards the cases presenting the greatest potential risk.

Q8 "When introducing AI in the selected application area, what is your organisation's starting point?"

The results provide a clear indication of how AI is currently being introduced into AML/CTF processes: 56% are augmenting an existing manual process, 33% are improving an existing tool, and 11% are building an entirely new process from scratch.

Figure 6: Starting point when introducing AI



> Organisations appear to be starting with established workflows and introducing AI where it can assist, accelerate or improve activities that are already being performed.

Only 11% of respondents say they are building an entirely new process from scratch.

This approach may offer practical advantages. Existing processes provide a known operating context, established controls and clearer reference points against which the performance of new technology can be evaluated.

It may also reduce some of the implementation risk associated with AI. Rather than simultaneously changing technology, process design and accountability structures, organisations can introduce AI into an existing operating model and develop experience before considering more substantial redesign.

Over time, this may change as organisations gain confidence in the technology and develop stronger data, governance and monitoring capabilities. The 2026 findings, however, indicate that AI adoption is currently more evolutionary than revolutionary.

Q9 "What are the biggest challenges your organisation faces when implementing AI in AML/CTF?"

The responses point primarily towards practical implementation barriers. The prominence of legacy-system integration as a key challenge suggests that the principal obstacles to AI adoption do not arise only from the capabilities or limitations of AI itself. They are also rooted in the technology environment in which AI needs to operate.

Figure 7: Biggest challenges when implementing AI in AML/CTF



AI applications within AML/CTF frequently depend on access to customer, transactional and risk information held across multiple systems. If that information cannot be accessed, combined or processed reliably, the practical value of AI will remain constrained regardless of the sophistication of the underlying technology.

The same applies to data quality and availability. More than half of respondents identify this as a challenge, reinforcing a wider finding of the survey: data capability is becoming central both to AMLR implementation and to the development of more technologically enabled financial crime prevention.

The results therefore point towards an important dependency: AI readiness is partly a function of existing organisational and technological maturity. Introducing an AI application does not remove weaknesses in data architecture, integration or underlying processes. In some cases, it may make those weaknesses more visible.

For AML and Compliance functions, selecting an AI use case is only one part of the implementation challenge. Organisations also need to assess whether the required data is available and reliable, whether existing systems can support integration, how performance will be measured, and how AI-enabled activities will fit within existing governance and accountability structures.

Respondents' Biggest Concerns About AI in Their Compliance Programmes

Respondents were also asked to describe, in their own words, their biggest concerns about AI implementation in their compliance programme.

> What concerns me most is how we make sure that AI supports our decisions in a way that is clear, fair, and easy to explain. We need to trust the underlying data, avoid hidden biases, and have solid governance so we always understand why the system reaches a certain conclusion."
>
> – Survey respondent

> That our organization will see a chance to not invest in agile third party tools but expect everything build in-house."
>
> – Survey respondent

> Lack of personnel with experience in how to develop and work with AI. We need a better understanding on what can be done through use of AI, how said things can be managed and understanding of limitations."
>
> – Survey respondent

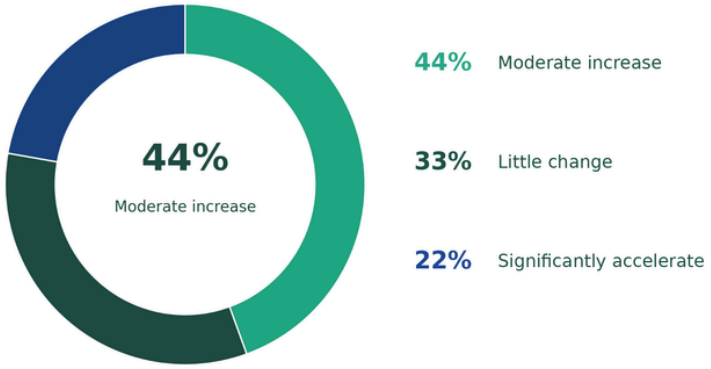
> Data quality and bias: AI models are only as good as the data they're trained on. If historical compliance data reflects biased enforcement or inconsistent categorization, the AI may replicate or amplify those problems. Explainability and auditability: Regulators and auditors often want to understand why a decision was made. Many AI systems (especially complex ML models) can act as "black boxes", making it hard to demonstrate sound reasoning behind a compliance decision. Regulatory uncertainty: The legal landscape around AI use in compliance is still evolving (the EU AI Act being a major example). Over-reliance and deskilling: There's a concern that teams may defer too heavily to AI outputs without applying professional judgment, which could erode institutional expertise over time."
>
> – Survey respondent

Q10 "How do you anticipate AMLR will impact your organisation's approach to using technology in compliance?"

AMLR is expected to strengthen the case for technology investment in compliance, although for most organisations the impact is likely to be incremental rather than transformative.

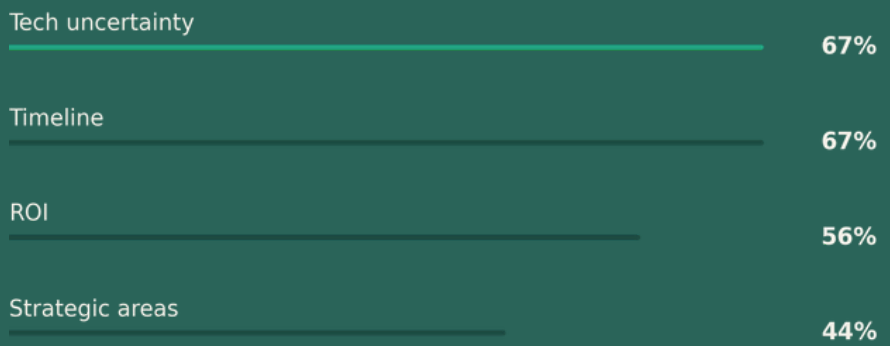
Two-thirds of respondents anticipate increased technology adoption or investment, with 44% expecting a moderate increase and 22% expecting a significant acceleration. A third expect little change to their existing technology plans.

Figure 8: Expected AMLR impact on the approach to technology in compliance



Q11 "What are your biggest concerns about AMLR implementation in relation to your technology/AI strategy?"

Figure 9: Biggest concerns about AMLR implementation in relation to technology/AI strategy



System limitations, IT development timelines and uncertainty around technology strategy stand out as potential blockers to successful AMLR implementation

The 2026 results reinforce a point which was made evident in our 2025 survey, namely that system limitations, IT development timelines and uncertainty around technology strategy stand out as potential blockers to successful AMLR implementation.

By way of comparison, our 2025 survey showed that lack of specific standards for AI in compliance ranked as the number one biggest concern at 28%, followed by balancing innovation with compliance at 22%. Uncertainty about which technology would meet the requirements and cost of compliance each accounted for 17%, while only 6% identified implementation timelines. The 2026 question permits multiple selections, so the percentages cannot be directly compared. However, the centre of concern appears to have moved towards execution.

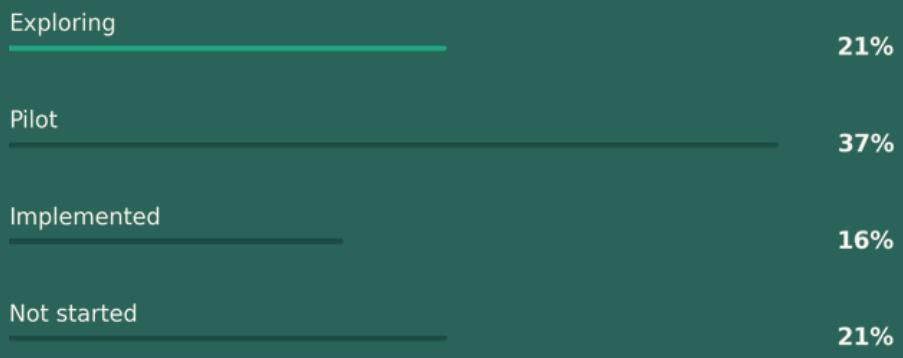
3. Technical Capabilities and AI Strategy As Enablers When Implementing the AMLR

Q12 "What is your organisation's current stage in AI adaption for compliance functions?"

The results point to a clear acceleration in AI adoption over the past year. In 2025, three-quarters of respondents were still either exploring AI or had not yet started, while only 17% had progressed to pilot projects. Now, pilot projects have become the largest category, increasing to 37%, while a further 16% report that AI solutions are already implemented in at least parts of their processes.



Figure 10: Current stage in AI adoption for compliance functions



This suggests that the market has moved beyond predominantly discussing and exploring AI towards practical experimentation and implementation. It has however not yet made the next transition to scaled, mature adoption. Nevertheless, adoption is far from mature: 21% have yet to start exploring AI and no respondents report advanced implementation with ongoing optimisation.

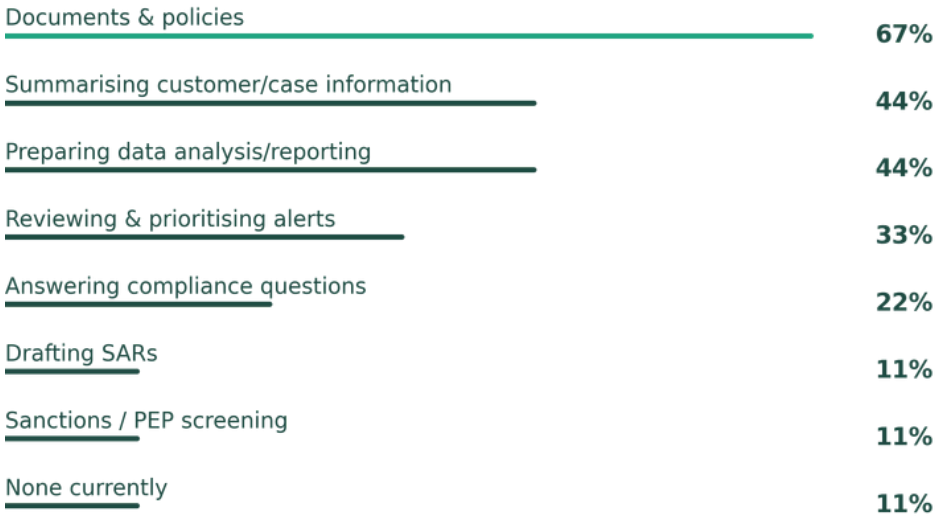
Q13 "In which of the following areas is AI currently helping your compliance or AML team?"

A natural starting point is to ask where AI is actually being used in day-to-day compliance and AML work today. Our results show that the most common applications are currently focused on supporting everyday information-intensive tasks. Searching through documents and policies leads the way, used by 67% of respondents, followed by summarising customer or case information and preparing data for analysis or reporting, both at 44%.

Use in more judgement-intensive AML processes remains less widespread. A third of respondents use AI to support the review and prioritisation of transaction monitoring alerts, while only 11% currently use it for drafting SARs or sanctions and PEP screening.

The pattern suggests a pragmatic adoption where AI is being deployed to reduce the information-processing burden on compliance teams, rather than to automate core AML decisions. Further, the question for AML leadership is what comes next, whether experience from these day-to-day applications will provide the confidence, governance and capabilities needed to deploy AI more deeply into core AML/CTF processes

Figure 11: Areas where AI is currently helping compliance and AML teams



> The clearest area of strength is drafting written summaries and reports. More than half of respondents with experience in this area say AI works well.

Q14 "Based on your experience, how well does AI perform in the following compliance tasks?"

The results provide a useful indication of where AI is currently delivering value in compliance and where human judgement remains difficult to replace. The clearest area of strength is drafting written summaries and reports. More than half of respondents with experience in this area say AI works well, making it the strongest-performing use case in the survey. AI also shows promise in identifying patterns across customers or transactions, although experiences are more mixed.

For several other tasks, adoption remains limited, but the experience of those already using AI is noteworthy. In alert prioritisation and explaining why transactions have been flagged, no respondents report that AI performs poorly; where it is being used, the assessment is generally positive.

A different picture emerges as tasks become more complex and judgement-intensive. AI is rarely used for handling unusual cases or making final decisions and recommendations, and no respondents say it works well in either area.

Figure 12: AI performance across compliance tasks

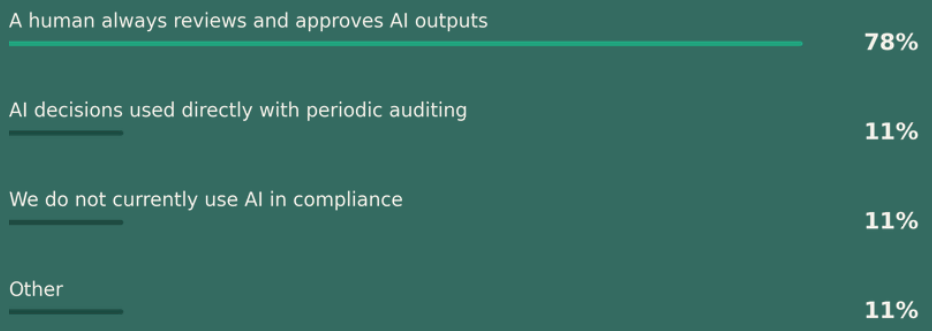
Compliance task	We don't use AI	Does not work well	Works partially	Works well	Overall signal
Drafting written summaries or reports	22%	0%	22%	56%	Strongest performance
Identifying patterns across customers or transactions	44%	11%	22%	22%	Promising, but mixed
Explaining why a transaction was flagged	63%	0%	13%	25%	Positive where used
Sorting or prioritising large volumes of alerts	75%	0%	0%	25%	Limited use, positive experience
Handling unusual or complex cases	75%	0%	25%	0%	Limited capability
Making final decisions or recommendations	88%	0%	13%	0%	Least suited / least adopted

Overall, the results suggest a relatively clear boundary in current AI capability: AI appears strongest when organising, analysing and summarising information, but considerably less mature when required to exercise judgement in complex or consequential decisions. For AML leadership, this reinforces the importance of viewing AI primarily as an augmentation tool at this stage, enhancing.

Q15 "How does your organisation involve humans in AI-supported compliance processes?"

Our results show that human oversight, human judgement and accountability remain firmly embedded in AI-supported compliance processes. Eight out of ten respondents state that a human always reviews and approves AI output before any action is taken. 11% report using AI decisions directly with periodic human auditing, while none limit human involvement solely to complex or high-risk cases. Respondents were asked to select all options that apply to them.

Figure 13: Human involvement in AI-supported compliance processes



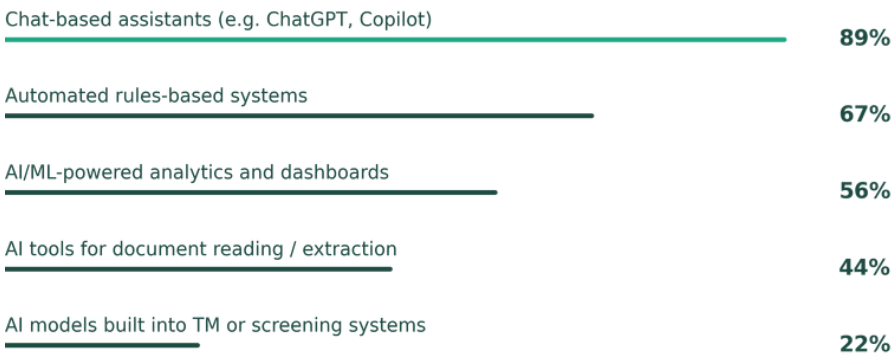
> Eight out of ten respondents state that a human always reviews and approves AI output before any action is taken.

This points to a cautious operating model in which AI is being used to support rather than replace human decision-making. Meanwhile, the results raise an important forward-looking question for AML leadership. As AI capabilities mature, will this level of human review remain sustainable or will institutions need to develop more risk-based models of human oversight? This is an issue which will likely have implications not only for efficiency, but also for governance, accountability and competence requirements.

Q16 "How would you describe the AI or technology tools your organisation uses (or is considering) in compliance?"

Respondents were asked to select all options that apply to them.

Figure 14: AI and technology tools used or considered in compliance



> Chat-based assistants are used or considered by 89% of respondents – many organisations are beginning their AI journey with readily accessible tools.

Chat-based assistants are used or considered by 89% of respondents, suggesting that many organisations are beginning their AI journey with readily accessible tools that can support a broad range of everyday compliance activities. The results also indicate the beginnings of a move towards more specialised applications.

More than half of respondents are using or considering AI/ML-powered analytics, 44% document-reading and data-extraction tools, while 22% are looking at AI embedded directly within transaction monitoring or screening systems.

The results raise a broader strategic question, whether the current dominance of general-purpose AI might simply be the starting point.

While general-purpose AI can provide broad productivity gains across the compliance function, specialised and increasingly embedded AI may address specific financial crime risks and processes where greater integration, control and domain expertise are required.

The strategic question going forward may therefore be more about where different forms of AI belong in the compliance architecture. Organisations will need to determine which capabilities can be served effectively by general-purpose tools and where purpose-built or embedded solutions are justified by the risk, complexity and potential value involved. This choice is likely to become an increasingly important part of the overall AI strategy that financial institutes strive to deliver on within AML.

Q17 "How has AI, as a tool or "co-worker", changed the way your compliance team works day-to-day?"

One-third of respondents say AI has meaningfully reduced time spent on repetitive tasks, making efficiency the most commonly reported benefit. A further 22% report improvements in the quality or consistency of their work, while 11% say AI has enabled their teams to handle greater volumes without increasing headcount.

Figure 15: How AI has changed day-to-day compliance work



We should nevertheless be cautious not to overstate the transformation. A third of respondents either do not yet use AI in their day-to-day compliance work or have seen no noticeable impact. As of now, the results suggest a market where the benefits are becoming visible but are not yet universal or transformational.

Perhaps most interesting for AML leadership is what this means for the next stage of adoption. The first wave of benefits appears to come from doing existing work faster and more consistently. The strategic opportunity ahead may be to move beyond productivity gains and consider how AI could change the operating model itself meaning how work is allocated between people and technology, which activities require specialist human judgement, and where increased capacity can be redirected towards higher-value investigative and risk-focused work.

In that sense, the longer-term question beyond "How much time can AI save?" is "What should compliance professionals do differently with the capacity AI creates?"

> Beyond "How much time can AI save?" the longer-term question is "What should compliance professionals do differently with the capacity AI creates?"

4. Future Outlook on AI in AML

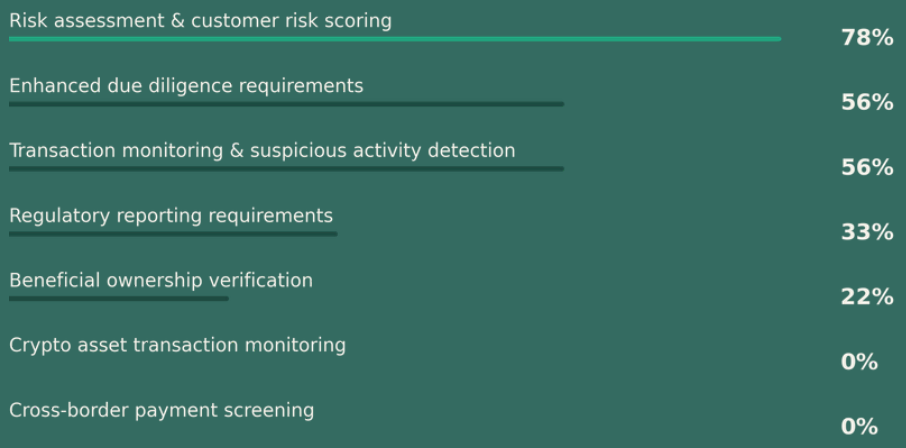
Q18 "Which aspects of AMLR compliance do you believe AI could most help your organisation address?"

In the 2025 survey, 100% selected transaction monitoring, followed by risk assessment and customer risk scoring at 65% and regulatory reporting at 47% as the principal application area for AI.

The 2026 survey asked respondents to select up to three areas where AI could most help address AMLR compliance. Transaction monitoring remains important, but risk assessment and customer risk scoring now emerges as the most frequently selected AI opportunity. Enhanced due diligence also features strongly.

This suggests that organisations increasingly see AI as relevant across the broader customer-risk lifecycle, including assessment, due diligence and information processing. This direction also fits the wider transformation agenda. Risk assessment, CDD and monitoring increasingly depend upon the same ability to integrate reliable data across processes rather than treating them as isolated controls.

Figure 16: Aspects of AMLR compliance where AI could help most

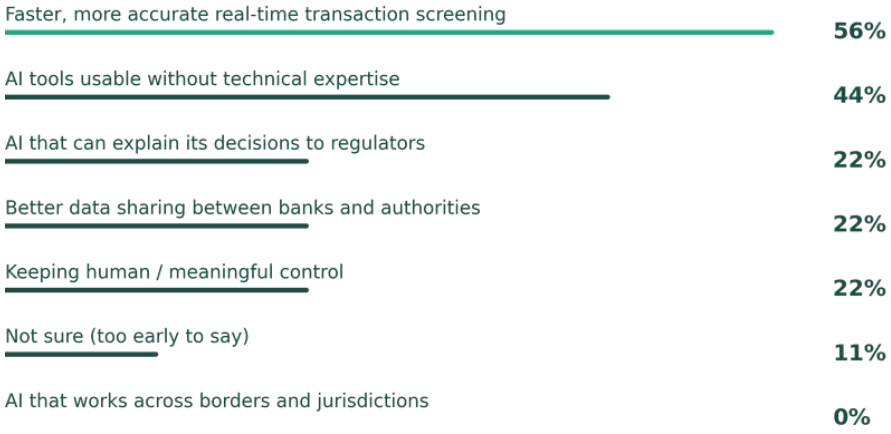


Risk assessment, CDD and monitoring increasingly depend upon the same ability to integrate reliable data across processes rather than treating them as isolated controls.

Q19 "Thinking about the next 2–3 years, which of the following do you think will matter most for how AI is used in financial crime prevention?"

Respondents were asked to select up to two options.

Figure 17: What will matter most for AI in financial crime prevention over the next 2–3 years



The results offer an indication of where AML professionals expect the next wave of AI value to come from. 56% of respondents opted for faster and more accurate real-time transaction screening. Another significant indication is the demand for AI tools that compliance professionals can use without technical expertise, which was identified by 44%.

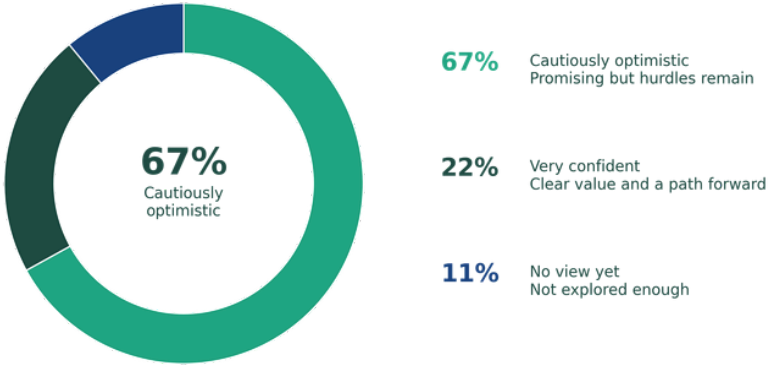
The combination of these two outputs suggests that the next stage of AI adoption may depend not only on more sophisticated technology, but on making that technology genuinely usable by compliance professionals. So long as AI remains dependent on scarce technical expertise, its ability to become embedded in day-to-day financial crime prevention may remain constrained.

Other priorities point towards the conditions required for broader adoption. Explainability to regulators and auditors, better data sharing between institutions and authorities, and maintaining meaningful human control were each identified by 22% of respondents. No respondents selected AI operating seamlessly across borders and legal jurisdictions, suggesting that immediate operational and usability challenges currently take precedence over more ambitious cross-border applications.

> For AML leadership, the message is therefore that the next phase of AI may be as much about accessibility, trust and integration as technological sophistication. The organisations that are able to drive competitive momentum, may be those that can put increasingly powerful capabilities directly into the hands of AML professionals while maintaining the explainability, governance and human oversight necessary to use them with confidence.

Q20 "How confident is your organisation that AI will be a net positive for your compliance program over the next 3 years?"

Figure 18: Confidence that AI will be a net positive over the next 3 years



The results point to positive but measured expectations for the future role of AI within AML. Two-thirds of respondents describe themselves as cautiously optimistic, recognising the potential of AI while also acknowledging that significant hurdles remain. A further 22% are very confident and see both clear value and a path forward, while 11% have yet to form a view.

In other words, optimism is accompanied by a healthy degree of caution. While none of the respondents selected the sceptical or uncertain alternatives, the majority answering "cautiously optimistic" indicates that confidence in AI's potential should not be confused with confidence in its implementation.

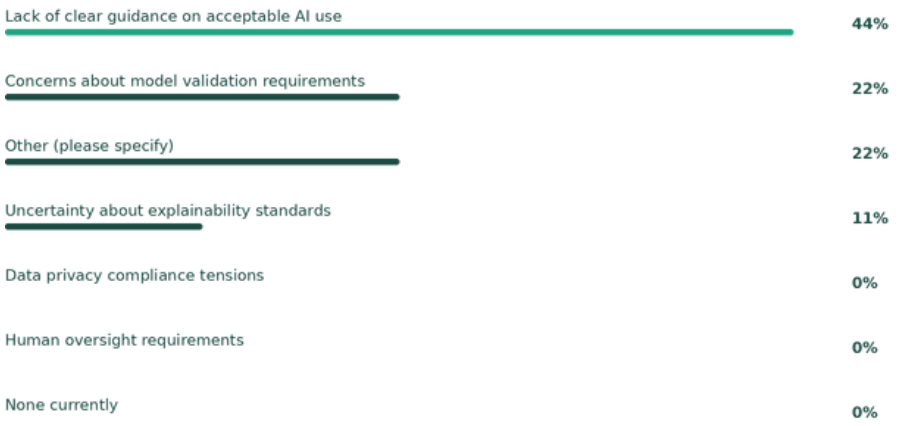
For AML leadership, this distinction is important. The challenge is increasingly about converting potential into practice, addressing governance, data, competence, regulatory expectations and human oversight in a way that allows AI to deliver sustainable value.

> The challenge is increasingly about converting potential into practice – addressing governance, data, competence, regulatory expectations and human oversight in a way that allows AI to deliver sustainable value.

Q21 "What concerns do you have about Swedish Financial Supervisory Authority expectations regarding AI use in compliance functions?"

Regulatory clarity is a key concern around AI use in compliance. The most frequently cited issue is a lack of clear guidance from the Financial Supervisory Authority on what constitutes acceptable AI use, selected by 44% of respondents. At 22%, concerns around model validation requirements follow, while 11% highlight uncertainty about explainability standards.

Figure 19: Concerns about FSA expectations regarding AI use in compliance



Notably, none of the respondents selected data privacy tensions, human oversight requirements or "no concerns" as their primary concern.

For AML leadership, the broader message is that the regulatory challenge is not necessarily opposition to AI, but uncertainty about the standards against which AI will be judged. Questions around acceptable use, validation and explainability all point in the same direction: organisations need greater confidence in how supervisors will assess AI-enabled compliance processes.

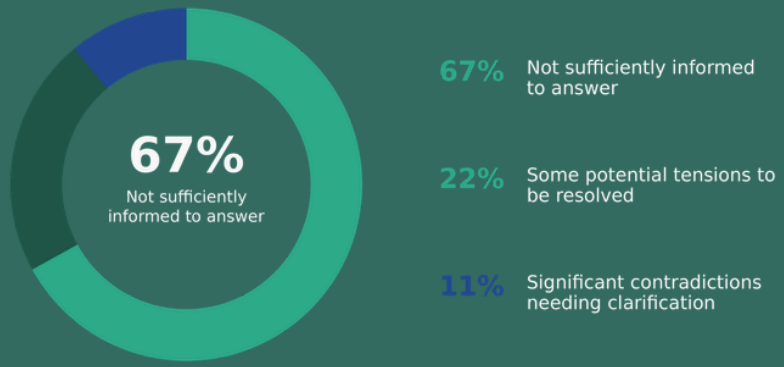
> This makes regulatory engagement an increasingly important part of AI strategy. Institutions may need to invest not only in the technology itself, but also in governance, documentation and validation frameworks that can demonstrate how AI is controlled, tested and used responsibly. In practice, progress may depend as much on building regulatory confidence as on improving technical capability.

Q22 "How do you perceive the alignment between Swedish regulatory expectations and the upcoming EU AI Act requirements for high-risk AI systems?"

As organisations increasingly explore and implement AI in compliance, understanding how different regulatory requirements interact will become an important part of effective AI governance. The results among respondents suggest that this understanding is not yet sufficiently developed.

Two-thirds of respondents state that they are not sufficiently informed to assess the alignment between the two regulatory frameworks. Among those expressing a view, 22% see potential tensions that need to be resolved, while 11% perceive more significant contradictions requiring clarification. No respondents consider the frameworks clearly aligned.

Figure 20: Perceived alignment between Swedish expectations and the EU AI Act





5. Advisense Perspective on AMLR and AI As Interconnected Investments

Successful AMLR implementation and scalable AI adoption depend on many of the same foundational capabilities. Both will necessitate organisations to progress from fragmented data and manual, siloed processes towards an environment in which reliable data can be accessed, combined and processed consistently and, where appropriate, in real time.

An institution that struggles to retrieve reliable AML data on demand will also struggle to provide AI applications with the trusted data required to operate effectively. Conversely, investment in data architecture, governance, traceability and integrated processes can serve two objectives simultaneously: strengthening AMLR readiness while creating the foundation on which more advanced analytics, automation and AI applications can be developed.

> An institution that struggles to retrieve reliable AML data on demand will also struggle to provide AI applications with the trusted data required to operate effectively.

This is particularly relevant given the increasing speed with which AI capabilities continue to develop. The opportunity is not simply to automate existing manual processes, but potentially to reconsider how elements of financial crime prevention are performed. At the same time, greater AI autonomy creates requirements around transparency, monitoring and accountability. Governance therefore needs to evolve alongside technological capability, with clear decisions about which activities that can appropriately be delegated to AI and where meaningful human judgement and accountability must remain.

The 2026 survey results should be viewed against this background. They indicate that institutions increasingly recognize the operational importance of data, technology and cross-functional implementation. Customer data management and KYC remediation are among the areas expected to experience the greatest operational impact from AMLR, while increased data-reporting obligations stand out as the most widely identified compliance challenge. At the same time, organisations are moving further into practical AI implementation.

Rather than viewing AMLR compliance and AI adoption as two independent programmes competing for investment, institutions have an opportunity to treat them as two outcomes of the same underlying transformation.

Making Transformation Deliverable

Approaching AMLR as a transformation opportunity needs to begin with an informed understanding of the organisation's starting point.

A useful first step is therefore to assess the current maturity of the AML organisation considering governance, processes, data and analytics, technology and people. The question asked is whether existing capabilities are able to accommodate to what a successful AMLR implementation will involve. This establishes where structural weaknesses already exist and helps prevent an AMLR programme from simply building new requirements on top of unresolved legacy issues.

The future state should then be defined together with those who will ultimately own and operate it. AMLR transformation will affect Compliance, business functions, technology, data and operations simultaneously. Effective implementation therefore requires cross-functional decision-making with sufficient mandate, rather than treating individual functions as downstream recipients of a centrally designed programme.

The organisational dimension is a critical factor overarching all else. New processes, technology and AI will change how people work

The organisational dimension is a critical factor overarching all else. New processes, technology and AI will change how people work. Employees affected by that change need to be involved early, particularly where automation or AI changes responsibilities or creates concerns about the future role of human judgement.

The strategic question is therefore broader than "How do we comply with the AMLR?" Financial institutions should also consider what they want their AML/CTF – and in the broader sense financial crime prevention – framework to look like towards 2030, and how the AMLR implementation programme can accelerate that journey.

Viewed in this way, July 2027 is not only a regulatory deadline. It creates a window in which organisations can address longstanding weaknesses in data, systems and fragmented processes while building a financial crime prevention framework better equipped for both a more data-driven supervisory environment and the opportunities created by AI.

6. Navigating the Next Phase

At a strategic level, the convergence of AMLR implementation and rapidly developing AI capability creates a broader question for management and boards. Over and beyond question of how to achieve regulatory compliance by July 2027, the broader issue is about what kind of financial crime prevention capability the organisation wants to have in place towards 2030, and how current AMLR investments can accelerate that development.

Advisense recommendations structured around seven steps to consider when navigating implementation:

1. Know where you stand before deciding where to go

AMLR transformation needs to begin with a clear understanding of the current AML/CTF maturity. The first step of an assessment needs to extend beyond formal regulatory compliance and consider the condition of the underlying operating model across:

- Governance
- Processes
- Data and analytics
- Technology
- People and organisational capability

This reflects the transformation principle that organisations should establish their starting point before defining the future state. Without this foundational assessment, investment decisions risk being based on assumptions and can result in failure and unnecessary rework.

2. Understand the data requirement early

With 100% of respondents identifying increased data-reporting obligations as a major compliance challenge, data should be treated as a foundational AMLR implementation workstream. Organisations need to understand:

- what data the future requirements will demand;
- where that data is currently held;
- whether it is sufficiently complete and reliable;
- whether lineage and audit traceability can be demonstrated;
- and whether existing systems can process and report it within required timelines.

This assessment should precede major technology decisions.

3. Test technical capacity against actual requirements

The 2026 survey shows that uncertainty about whether technology will meet AMLR requirements is now one of the most frequently cited implementation concerns. A maturity or gap assessment should therefore evaluate not only legal compliance, but the capacity of the current architecture to support future processes.

This includes legacy-system constraints, data integration, reporting capabilities and whether existing technology contains functionality that is currently underutilised.

4. Define the destination with the people who will own it

A common practice is to have a small central project group developing the future operating model. To be successful, those who will ultimately operate the processes, systems and controls need to be actively involved from the start and contribute to defining the target state. Doing so builds ownership early and reduces the risk that the strategy becomes disconnected from operational reality.
This is particularly important where AMLR implementation changes responsibilities across Compliance, first line, operations, IT and data functions.

5. Treat organisational capacity as an implementation constraint

AMLR implementation will compete with business-as-usual responsibilities for compliance, legal, technology and data resources. The question is therefore not merely what changes are required, but whether the organisation possesses the capacity to deliver those changes while maintaining current compliance obligations.

Cross-functional planning, management sponsorship, sufficient budget and realistic technology-development timelines should be established early. The previous report described capacity in terms of personnel, skillsets, systems and technical capabilities. That definition remains highly relevant to the 2026 findings.

6. Put decision-making mandate where it is needed

Cross-functional participation is key but in itself insufficient. Programme governance needs to have the necessary authority or mechanisms to resolve dependencies, align competing priorities, and address issues that span multiple functions.

Financial crime transformation affects business divisions, technology, compliance and operations simultaneously. Steering and governance structures therefore need people who possess the mandate to make binding decisions across these areas, rather than relying on seniority alone.

7. Treat change management as part of implementation

The organisational impact should not be underestimated. New technology, automation and AI can change both workflows and roles. Organisations therefore need to communicate early, engage with affected employees and address concerns about how responsibilities and human judgement will evolve.

Successful transformation requires strategy, execution, performance and risk management, and stakeholder and change management to move together, rather than treating organisational change as a supporting activity once technical implementation has already been completed.



Contact

Daniel Bardun
Senior Manager, Financial Crime Prevention
daniel.bardun@advisense.com
+467 081 853 42

Jonas Karlsson
Managing Director, Financial Crime Prevention
jonas.karlsson@advisense.com
+467 217 949 83


advisense