WHITE PAPER

SymphonyAI

Technology readiness for AMLA

Five technology foundations every MLRO should be evaluating

Executive summary

The establishment of the European Anti-Money Laundering Authority (AMLA) marks the beginning of a new era for financial crime compliance in Europe. Together with the EU AML Regulation and AMLD6, AMLA introduces a more harmonized regulatory framework designed to strengthen supervisory consistency across the European Union [1][2][3]. In our view, this evolution also changes the technology foundations required to deliver consistent, effective, and demonstrable compliance.

For many financial institutions, AMLA represents a shift in perspective. Historically, AML transformation programs have centered on implementing regulatory change through policies, procedures, and governance frameworks. While these remain essential, the focus is increasingly moving toward the operational capabilities that enable institutions to apply those requirements consistently, adapt to evolving regulatory expectations, and demonstrate effectiveness to supervisors [2][3].

This evolution changes the role of technology. Compliance platforms are increasingly expected to enable continuous risk assessment, provide transparent and auditable decision-making, improve data quality, strengthen enterprise-wide governance, and support harmonized reporting across jurisdictions. With AMLA now finalizing key private-sector Regulatory Technical Standards (RTS), while continuing to develop further RTS, Implementing Technical Standards (ITS), and Guidelines, technology will become an increasingly important enabler of regulatory consistency and operational resilience [5][6][7][10][13].

AMLA's new standards represents a significant evolution in the technology capabilities needed to support financial crime compliance across Europe.

The challenge for compliance leaders is to build technology foundations that can evolve alongside the regulatory framework and support consistent, transparent, and demonstrably effective compliance over time.

This guide explores five technology priorities that we believe every MLRO and senior financial crime leader should be evaluating today:

1. Continuous customer risk monitoring
2. Enterprise data readiness
3. AI-assisted investigations
4. Integrated financial crime intelligence
5. Governance, reporting, and auditability

These priorities represent the foundational technology capabilities that will increasingly distinguish organizations that are prepared for AMLA's initial implementation, as well as for the continuous regulatory evolution that will follow.

At a glance

AMLA Technology Readiness

Building the technology foundations for harmonized, effective financial crime compliance

WHY AMLA MATTERS

The establishment of AMLA and the EU AML Package mark the beginning of a more harmonized regulatory approach to financial crime compliance across the European Union.

As AMLA develops RTS, ITS, and supervisory Guidelines, institutions will need technology capable of supporting consistent implementation, transparent decision-making, and demonstrable compliance.

Technology readiness is therefore becoming an increasingly important component of regulatory readiness.

AMLA IS DRIVING A SHIFT FROM...

TRADITIONAL COMPLIANCE		AMLA-READY COMPLIANCE
Periodic customer reviews	›	**Continuous customer risk monitoring**
Siloed financial crime functions	›	**Connected enterprise intelligence**
Fragmented data	›	**Trusted enterprise data**
Manual investigations	›	**AI-assisted investigations**
Static compliance processes	›	**Adaptive, technology-enabled compliance**
Reactive reporting	›	**Transparent governance and auditability**

THE STRATEGIC QUESTION FOR MLROS **"Does your technology enable you to respond confidently to today's re-equipment and tomorrow's supervisory expectations?"**

FIVE TECHNOLOGY FOUNDATIONS FOR AMLA AND WHY THEY MATTER

1. **Continuous customer risk monitoring**
   Maintain an up-to-date understanding of customer risk throughout the business relationship
2. **Enterprise data readiness**
   Provide trusted, connected, and accessible data to support consistent compliance decisions
3. **AI-assisted investigations**
   Improve investigation quality and operational efficiency while maintaining human oversight
4. **Integrated financial crime and fraud intelligence**
   Connect information across customer due diligence, monitoring, screening, investigations, and reporting
5. **Governance, reporting, and auditability**
   Demonstrate transparent, explainable, and consistent compliance to regulators and supervisors

COMMON TECHNOLOGY CHALLENGES

Fragmented data
Financial crime data resides across multiple systems, reducing visibility and increasing reconciliation effort

Legacy technology
Older systems can limit agility and make adapting to new requirements complex and costly

Manual processes
High levels of manual work limit capacity and increase the risk of inconsistency and error

Limited enterprise visibility
Siloed systems and teams can lead to incomplete views of risk across the organization

Adapting to regulatory change
Ongoing evolution of RTS, ITS, Guidelines, and supervisory expectations requires continuous adaptation

THE FUTURE-READY OUTCOME

CONSISTENT
Apply controls consistently across jurisdictions and business lines

TRANSPARENT
Provide clear, explainable, and evidence-based decisions

CONNECTED
Integrate data and intelligence across the financial crime lifecycle

ADAPTIVE
Evolve technology capabilities with regulatory and business change

EFFECTIVE
Deliver measurable outcomes and stronger supervisory confidence

AMLA marks a new era for financial crime compliance

The establishment of the AMLA is more than an institutional reform. It signals a fundamental shift in how anti-money laundering and counter-terrorist financing (AML/CFT) supervision will be delivered across the European Union. Rather than relying on 27 national interpretations of common legislation, AMLA introduces a harmonized regulatory framework designed to promote supervisory convergence, consistent implementation, and higher standards of effectiveness across member states [1][2].

This change reflects a broader objective of the EU AML Package. The focus is on creating a more consistent, transparent, and effective AML/CFT framework across the single market. The introduction of directly applicable regulations, supported by Regulatory Technical Standards (RTS), Implementing Technical Standards (ITS), and supervisory Guidelines (GL), is intended to reduce regulatory fragmentation and establish a common supervisory baseline for all obligated entities [2][3].

For compliance leaders, this represents an important shift. Historically, many financial institutions have designed their AML technology around local regulatory expectations, individual business lines, or jurisdiction-specific operating models. While these approaches may have satisfied national requirements, they often resulted in fragmented data, inconsistent controls, and varying interpretations of regulatory obligations. It also meant different legal entities in different countries had different setups, configurations, controls and views of the same or similar counterparties.

AMLA raises the expectation for greater operational consistency. The Authority has now finalized several key technical standards covering customer due diligence, the identification of business relationships and occasional and linked transactions, and group-wide AML/CFT requirements, while further regulatory instruments continue to develop [5][7][10][13].

Institutions will need technology capable of applying these requirements consistently across jurisdictions and adapting as the Single Rulebook continues to evolve.

Technology therefore becomes a strategic enabler of regulatory compliance rather than a supporting function. The ability to maintain high-quality data, automate risk-based decision-making, provide transparent audit trails, and rapidly implement new regulatory requirements will increasingly determine how effectively institutions respond to AMLA's evolving supervisory framework.

For MLROs, the strategic question is whether today's technology foundations are sufficiently adaptable to support the next generation of European AML supervision.

From regulatory readiness to technology readiness

For many financial institutions, AML readiness has traditionally focused on regulatory interpretation. Programs have centered on understanding new legislation, updating policies and procedures, strengthening governance frameworks, and implementing the controls necessary to achieve compliance.

These activities remain essential. However, they represent only one dimension of AMLA readiness. As AMLA progressively builds out the European Single Rulebook through finalized standards, and guidelines, the challenge increasingly shifts from interpreting regulatory requirements to implementing them consistently across the enterprise. Compliance will increasingly depend on governance and policy, together with the technology foundations that enable institutions to operationalize regulatory expectations at scale [2][5][6].

The questions compliance leaders should be asking:

- Can we continuously assess customer risk as new information becomes available?
- Can we apply controls consistently across jurisdictions, business lines, and legal entities?
- Can we explain and evidence how risk decisions were reached?
- Can we produce standardized, accurate, and timely regulatory reporting?
- Can our technology adapt as AMLA publishes new standards and guidelines, and supervisory expectations?

These are fundamentally technology questions about building operational capabilities that support consistency, transparency, and agility in an evolving regulatory environment.

This is particularly important because AMLA is not a one-time regulatory event. The authority has an extensive mandate to develop technical standards, issue supervisory guidelines, and promote convergence across member states over the coming years [5][6].

Institutions therefore need technology that can evolve alongside the regulatory framework rather than requiring significant redesign each time new requirements emerge.

Technology readiness should therefore be viewed as a strategic capability rather than an implementation project. Institutions that invest in adaptable data, intelligence, and governance foundations will be able to respond to AMLA's initial requirements, and the continuous evolution of European AML supervision with ease.

Figure 1. From regulatory readiness to technology readiness

REGULATORY READINESS	TECHNOLOGY READINESS
Understand new legislation	Operationalize regulatory requirements consistently
Update policies and procedures	Enable continuous risk assessment
Strengthen governance	Embed controls across the enterprise
Interpret legal obligations	Produce transparent and explainable decisions
Implement one-time change	Adapt continuously to evolving RTS and Guidelines

Five technology priorities every MLRO should be evaluating

The EU AML Package does not prescribe specific technologies. It defines regulatory outcomes that financial institutions must achieve through effective governance, risk management, customer due diligence, ongoing monitoring, and reporting. As AMLA finalizes key regulatory instruments and continues to develop further RTS, ITS, and Guidelines, institutions will need technology capable of supporting these outcomes consistently, transparently, and at scale [2][5].

Based on the direction of the EU AML framework and SymphonyAI's experience supporting financial institutions globally, we believe five technology foundations will increasingly distinguish organizations that are prepared for AMLA's implementation and for its continued regulatory evolution.

These priorities should not be viewed as independent technology initiatives. Together, they form the foundation of a modern financial crime compliance architecture, capable of adapting as supervisory expectations continue to evolve.

Priority 1

Continuous customer risk monitoring

Why it matters

AMLA is bringing greater specificity to how customer due diligence requirements should be applied in practice. The finalized CDD RTS Article 28(1) sets out requirements around the information obliged entities must collect and verify, while the finalized RTS under Article 19(9) establishes criteria for identifying business relationships, occasional transactions, and linked transactions. Alongside AMLA's developing Guidelines on ongoing monitoring (Article 26(5)), these instruments reinforce the need for institutions to maintain an accurate and current understanding of customer risk throughout the business relationship [7][8][13].

This increases the importance of technology capable of maintaining current customer information, identifying relevant changes, and supporting timely risk reassessment rather than relying solely on scheduled reviews or manual intervention.

Current challenges

Many institutions continue to rely on periodic KYC reviews, fragmented customer data, and manual processes to identify changes in customer risk. These approaches often result in inconsistent risk assessments, delayed remediation, and increased operational effort.

As customer volumes grow and regulatory expectations evolve, maintaining current and accurate customer risk profiles becomes increasingly difficult without greater automation.

Technology considerations

Compliance leaders should evaluate whether existing technology can:

- Continuously refresh customer risk profiles as new internal or external information becomes available.
- Consolidate customer data from multiple systems into a consistent enterprise view.
- Trigger risk reassessments automatically based on predefined events.
- Support consistent customer risk methodologies across jurisdictions.
- Maintain complete audit trails for every risk assessment and decision.

QUESTIONS FOR MLROS

- How quickly do you identify changes in customer risk?
- Which customer risk assessments remain dependent on manual review?
- Can you demonstrate why a customer's risk rating changed?
- Can you apply consistent customer risk methodologies across all jurisdictions?

Key takeaway

AMLA strengthens expectations around ongoing customer due diligence. Technology should enable institutions to identify relevant changes and reassess customer risk when needed, rather than relying solely on periodic reviews.

Figure 2. From periodic reviews to continuous risk monitoring

TRADITIONAL APPROACH	TECHNOLOGY EVOLUTION
Periodic KYC reviews	**Continuous customer risk monitoring**
Manual risk updates	**Automated risk reassessment**
Multiple customer records	**Enterprise customer view**
Static customer profiles	**Dynamic risk profiles**
Reactive remediation	**Event-driven monitoring**

Priority 2

Enterprise data readiness

Why it matters

A harmonized regulatory framework depends on consistent, reliable, and accessible data. Across the EU AML Regulation and AMLA's developing and finalized regulatory instruments, there is a clear emphasis on accurate customer information, effective risk assessment, group-wide consistency, and standardized reporting [2][7][9][10][11][13]. These outcomes cannot be achieved if critical financial crime data remains fragmented across systems, jurisdictions, or business units [2][3][9][10].

As institutions prepare for AMLA, data readiness becomes more than a technology initiative. It becomes a prerequisite for effective compliance.

Current challenges

Many financial institutions continue to operate with fragmented customer, transaction, screening, and case management data spread across multiple platforms.

Differences in data standards, inconsistent identifiers, duplicate records, and manual reconciliation can reduce the quality of risk assessments and make enterprise-wide oversight more difficult.

These challenges are often amplified in multinational organizations, where different business units and jurisdictions have evolved independently over time.

Technology considerations

Compliance leaders should evaluate whether their technology can:

- Create a consistent enterprise view of customers, counterparties, and related entities.
- Maintain high-quality, standardized data across jurisdictions and business lines.
- Support lineage and traceability for regulatory reporting and supervisory review.
- Integrate customer, transaction, sanctions, and investigation data into a common compliance ecosystem.
- Adapt data models as AMLA introduces new reporting requirements and technical standards.

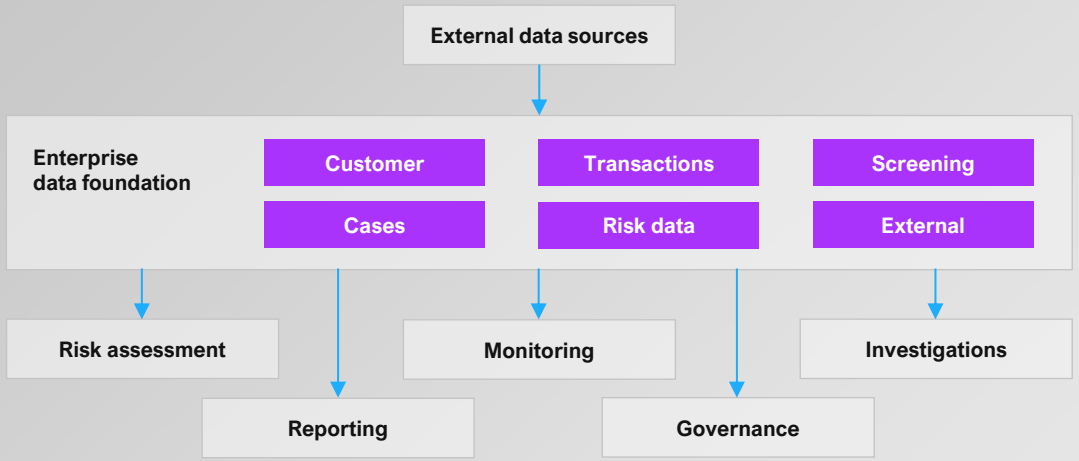
QUESTIONS FOR MLROS

- Can you establish a single, trusted view of customer risk across the organization?
- How much manual effort is required to reconcile data between systems?
- Can you demonstrate the origin, quality, and lineage of the data supporting regulatory decisions?
- How quickly can you incorporate new regulatory data requirements into your existing architecture?

Key takeaway

Technology readiness begins with data readiness. Trusted, connected, and well-governed data foundations will help institutions apply requirements consistently and adapt as AMLA's regulatory framework evolves.

Figure 3. Building an enterprise data foundation



Priority 3 AI-assisted Investigations

Why it matters

AMLA places increasing emphasis on effectiveness, consistency, and demonstrable decision-making. While investigations will continue to require expert judgment, the volume and complexity of alerts generated by modern financial crime programs make manual investigation models increasingly difficult to sustain.

AI has the potential to improve investigator productivity by automating repetitive tasks, consolidating information from multiple sources, generating case summaries, and supporting more consistent decision-making. As adoption increases, institutions will also need appropriate governance, transparency, and human oversight to ensure AI is used responsibly and in line with regulatory expectations [2][4][12].

Current challenges

Investigation teams continue to spend significant time collecting information from multiple systems, documenting findings, and preparing case files. Manual processes can lead to inconsistent investigations, longer case resolution times, and reduced capacity to focus on higher-risk activity. As alert volumes continue to increase, these operational constraints become increasingly difficult to manage without greater automation.

Technology considerations

Compliance leaders should evaluate whether investigation platforms can:

- Consolidate customer, transaction, sanctions, and case information into a single investigative workspace.
- Prioritize alerts based on risk and supporting evidence.
- Generate explainable summaries and recommended next steps.
- Maintain complete audit trails of investigator and AI-assisted activities.
- Support human review and approval throughout the investigation lifecycle.

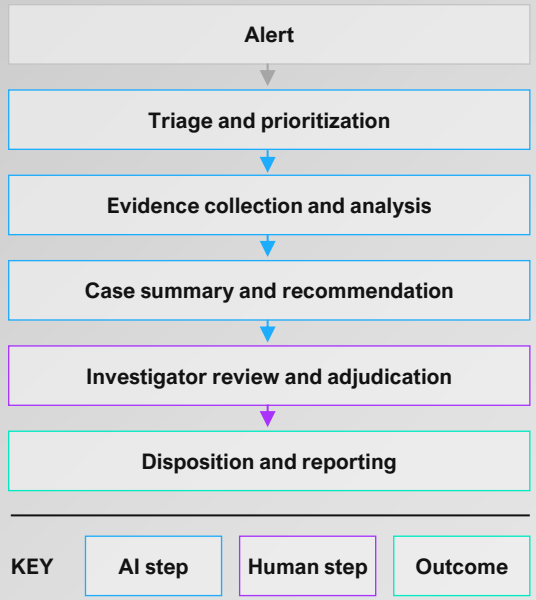
QUESTIONS FOR MLROS

- Where do investigators spend the greatest proportion of their time?
- Which investigation activities could be safely automated?
- Can you explain how AI-generated recommendations were produced?
- How do you ensure investigators remain accountable for final decisions?

Key takeaway

AI should enhance investigator expertise, not replace it. Institutions combining AI-assisted workflows with strong governance and human oversight can improve operational efficiency while maintaining transparency and accountability.

Figure 4. AI-assisted investigation workflow - AI as an enabler within a human-led investigation process, reinforcing explainability and accountability.



Priority 4 Integrated FinCrime and fraud intelligence

Why it matters

Financial crime rarely occurs in isolated processes. Customer due diligence, transaction monitoring, sanctions screening, investigations, payment fraud and regulatory reporting each provide valuable risk indicators, yet many institutions continue to manage these activities independently.

AMLA's emphasis on harmonized supervision and consistent application of AML/CFT controls is reinforced by the finalized RTS on group-wide requirements – Articles 16(4) and 17(3), which sets minimum requirements for group-wide governance, risk management, internal controls, and secure information sharing [2][10]. For complex financial groups, this increases the importance of technology that can connect relevant financial crime data and intelligence across entities and jurisdictions while supporting consistent group-wide oversight.

Current challenges

Many organizations continue to operate separate platforms for KYC, transaction monitoring, sanctions screening, adverse media, fraud, investigations, and reporting. While these systems often perform their individual functions effectively, they may not provide a consolidated view of financial crime risk across the customer lifecycle. This fragmentation can lead to duplicate investigations, inconsistent risk assessments, limited visibility across business lines, and missed opportunities to identify emerging risk patterns.

Technology considerations

Compliance leaders should evaluate whether their technology can:

- Connect intelligence from customer due diligence, transaction monitoring, sanctions, fraud, investigations, and reporting.
- Provide a consolidated enterprise view of customer and entity risk.
- Correlate risk indicators across multiple financial crime domains.
- Reduce duplicate investigations and improve operational coordination.
- Support enterprise-wide management information and risk reporting.

QUESTIONS FOR MLROS

- Can you view financial crime risk holistically, or only through individual systems?
- Are investigators able to access all relevant intelligence from a single workspace?
- How often are similar risks investigated separately by different teams?
- Can senior management obtain an enterprise-wide view of financial crime exposure?

Key takeaway

AMLA encourages a more consistent and coordinated approach to financial crime compliance. Technology should enable institutions to connect intelligence across functions rather than managing risk in isolated operational silos.

Figure 5. From functional silos to integrated financial crime intelligence

TRADITIONAL OPERATING MODEL	INTEGRATED INTELLIGENCE MODEL
Separate KYC platform	**Connected customer intelligence**
Independent transaction monitoring	**Shared enterprise risk view**
Standalone sanctions screening	**Cross-domain risk correlation**
Multiple investigation teams	**Unified investigation workflow**
Fragmented management reporting	**Enterprise financial crime intelligence**

Priority 5 Governance, reporting, and auditability

Why it matters

Under AMLA, governance is increasingly supported by standardized regulatory expectations, greater supervisory consistency, and a stronger emphasis on demonstrating how compliance decisions are made.

The finalized group-wide RTS adds further specificity around governance, risk management, internal controls, and information sharing across groups [10]. Institutions will need to evidence not only that appropriate controls exist, but also that they operate consistently, are supported by reliable data, and can withstand supervisory scrutiny. Technology therefore plays an increasingly important role in providing transparency, traceability, and accountability across the compliance lifecycle [1][2][10].

Current challenges

Many governance activities remain highly manual. Compliance teams often rely on spreadsheets, fragmented reporting, and time-consuming evidence gathering to demonstrate control effectiveness or respond to regulatory requests. As regulatory expectations become more standardized, these approaches can become increasingly difficult to scale while maintaining consistency and transparency.

Technology considerations

Compliance leaders should evaluate whether their technology can:

- Maintain complete audit trails for customer risk assessments, alerts, investigations, and reporting.
- Support explainable and traceable decision-making across automated and manual processes.
- Produce consistent management information and regulatory reporting.
- Monitor key operational and compliance performance indicators in near real time.
- Adapt reporting frameworks as AMLA introduces new technical standards and supervisory expectations.

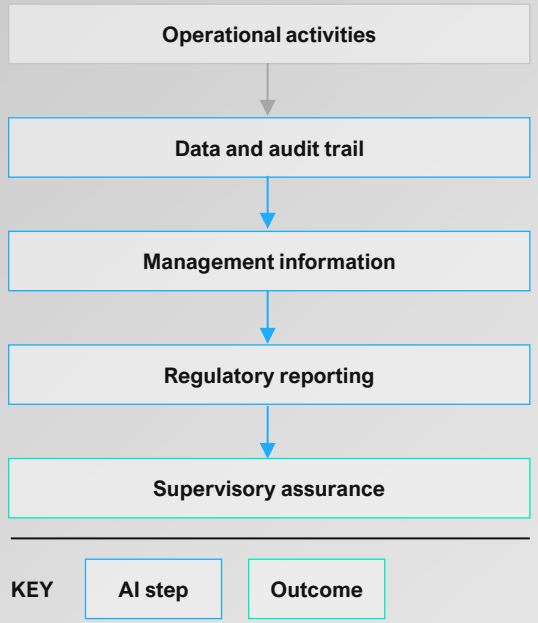
QUESTIONS FOR MLROS

- Can you demonstrate how significant compliance decisions were reached?
- How quickly can you respond to regulatory information requests?
- Are management reports generated consistently across the organization?
- Do you have complete auditability across your end-to-end compliance processes?

Key takeaway

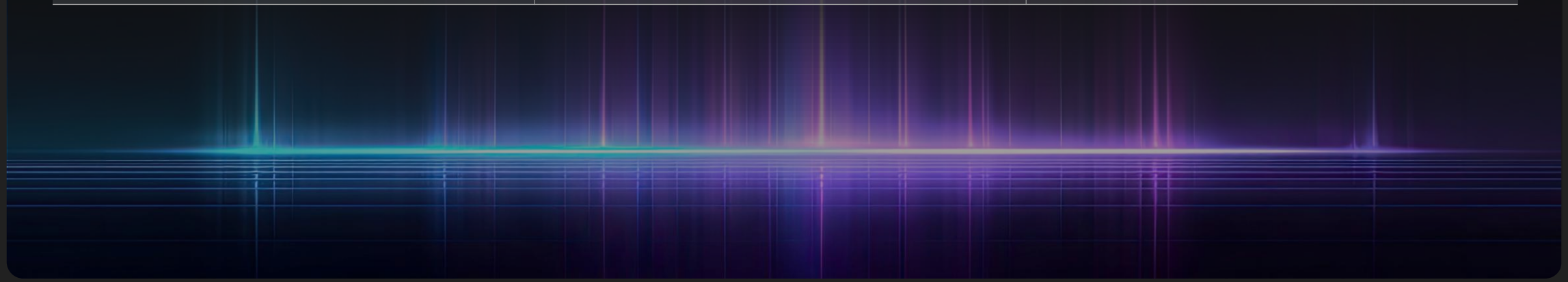
Technology should enable governance. Institutions with transparent, auditable, and adaptable governance capabilities will demonstrate compliance more effectively and respond confidently to evolving supervisory expectations.

Figure 6. Technology-enabled governance



THE FIVE TECHNOLOGY FOUNDATIONS FOR AMLA

Technology foundation	Primary objective	Regulatory outcome
Continuous customer risk monitoring	Maintain dynamic customer risk	Effective ongoing CDD
Enterprise data readiness	Create trusted, connected data	Consistent enterprise risk assessment
AI-assisted Investigations	Improve investigation quality and efficiency	Explainable, evidence-based decisions
Integrated FinCrime and Fraud Intelligence	Connect intelligence across compliance functions	Enterprise-wide risk visibility
Governance, reporting, and auditability	Demonstrate consistent compliance	Supervisory transparency and accountability



Common technology challenges financial institutions should address now

Most financial institutions have invested significantly in AML and financial crime technology over many years, often in response to evolving regulations, acquisitions, and changing business priorities. As a result, many compliance environments consist of multiple systems, data sources, and operational processes that have developed incrementally over time.

While these environments may meet today's regulatory requirements, AMLA's emphasis on harmonization, consistency, and demonstrable effectiveness encourages compliance leaders to consider whether existing technology foundations are sufficiently adaptable for the future.

Rather than viewing AMLA as a technology replacement programme, organizations are likely to focus on strengthening existing capabilities, improving integration, and modernizing areas where operational complexity creates unnecessary risk.
Across the industry, five challenges continue to emerge.

Fragmented data environments

Financial crime data often resides across multiple customer, transaction, sanctions, case management, and reporting systems. Fragmented data can reduce operational visibility, increase manual reconciliation, and make it more difficult to produce consistent regulatory outcomes.

Legacy technology constraints

Many AML platforms were implemented to address specific regulatory requirements at a point in time. As expectations evolve, adapting legacy systems to support new regulatory standards, reporting obligations, or analytical capabilities may become increasingly complex and costly.

Manual compliance processes

Customer reviews, investigations, reporting, and governance activities frequently rely on manual intervention. While expert judgment remains essential, repetitive administrative work can limit capacity for higher-value investigative and analytical activities.

Limited enterprise visibility

Financial crime risks rarely align with organizational structures. Separate systems and operational teams can make it difficult to establish a comprehensive view of customer risk across jurisdictions, business lines, and financial crime disciplines.

Adapting to continuous regulatory change

AMLA represents the beginning of a new European supervisory model. As finalized standards move through the EU adoption process and further RTS, ITS, Guidelines, and recommendations continue to develop, institutions will need technology that can adapt without requiring extensive redesign for every regulatory change [5].

For many institutions, AMLA readiness will depend on creating a more connected, adaptable, and transparent technology foundation capable of evolving alongside regulatory expectations.

Preparing for an evolving regulatory landscape

AMLA's regulatory program is moving progressively from framework development toward implementation. The finalization of key private-sector standards provides greater clarity around customer due diligence, business relationships and occasional and linked transactions, and group-wide AML/CFT requirements. These standards have been submitted to the European Commission and, once adopted and published in the Official Journal, are proposed to apply six months after entry into force [7][10][13].

At the same time, the Single Rulebook remains a work in progress. Further RTS, ITS, Guidelines, and other regulatory instruments will continue to shape how the EU AML framework is implemented in practice over the coming years[5][6].

For compliance leaders, technology readiness should therefore be viewed as an ongoing capability rather than a one-time implementation project. Institutions should establish flexible technology foundations capable of adapting as requirements and supervisory expectations evolve.

About this guide

This guide presents SymphonyAI's perspective on the technology implications of the EU AMLA and the wider EU AML Package.

It is intended to support strategic discussion among MLROs, compliance leaders, and financial crime professionals. The guide reflects publicly available legislation, AMLA consultation papers, and regulatory publications available at the time of writing. It does not constitute legal or regulatory advice.

Key regulatory sources

European Union legislative framework

[1] European Parliament and Council of the European Union. Regulation (EU) 2024/1620 of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010. Official Journal of the European Union, 19 June 2024.

[2] European Parliament and Council of the European Union. Regulation (EU) 2024/1624 of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Official Journal of the European Union, 19 June 2024.

[3] European Parliament and Council of the European Union. Directive (EU) 2024/1640 of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849. Official Journal of the European Union, 19 June 2024.

[4] European Parliament and Council of the European Union. Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonized rules on artificial intelligence and amending certain Union legislative acts. Official Journal of the European Union, 12 July 2024.

AMLA strategy and regulatory program

[5] European Anti-Money Laundering Authority. Regulatory Instruments. Consolidated overview of AMLA's Regulatory Technical Standards, Implementing Technical Standards, Guidelines, Recommendations, and related consultations under the EU AML/CFT framework.

[6] European Anti-Money Laundering Authority. Single Programming Document 2026–2028. AMLA, 2026.

Customer due diligence and ongoing monitoring

[7] European Anti-Money Laundering Authority. Final Report – Draft Regulatory Technical Standards under Article 28(1) of Regulation (EU) 2024/1624: Customer Due Diligence. 1 October 2026.

[8] European Anti-Money Laundering Authority. Consultation Paper on Draft Guidelines under Article 26(5) of Regulation (EU) 2024/1624: Ongoing Monitoring of Business Relationships. 3 June 2026.

Enterprise risk, group-wide consistency, and information sharing

[9] European Anti-Money Laundering Authority. Consultation Paper on Draft Guidelines under Article 10(4) of Regulation (EU) 2024/1624: Business-Wide Risk Assessment. 16 April 2026.

[10] European Anti-Money Laundering Authority. Final Report – Draft Regulatory Technical Standards under Articles 16(4) and 17(3) of Regulation (EU) 2024/1624: Group-Wide Minimum Requirements and Additional Measures for Subsidiaries and Branches in Third Countries. 1 October 2026.

Reporting and data standardization

[11] European Anti-Money Laundering Authority. Consultation Paper on Draft Implementing Technical Standards under Article 69(3) of Regulation (EU) 2024/1624: Format for Reporting Suspicions and Providing Transaction Records. 2 July 2026.

International standards

[12] Financial Action Task Force. International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations. Current consolidated edition.

[13] European Anti-Money Laundering Authority. Final Report – Draft Regulatory Technical Standards under Article 19(9) of Regulation (EU) 2024/1624: Criteria for Identifying Business Relationships, Occasional and Linked Transactions and Lower Thresholds. 1 October 2026.

SymphonyAI helps financial institutions modernize the technology foundations that support AMLA readiness. Our capabilities span customer due diligence and lifecycle risk management, screening and transaction monitoring, connected customer, transaction and entity intelligence, investigations and regulatory reporting, and transparent governance and auditability.

Through AI, advanced analytics and intelligent automation – with human oversight embedded into decision-making – we help institutions apply risk-based controls more consistently, improve operational effectiveness, and adapt as regulatory requirements evolve.

SymphonyAI

Authors



Charmian Simmons

Principal Strategic Advisor
FinCrime Compliance
SymphonyAI



Lala Huseynli

Financial Services Marketing
and Growth Lead, EMEA
SymphonyAI

Get in touch with us today to discuss your AMLA technology priorities and how SymphonyAI can support your technology readiness journey.

Email connect.fs@symphonyai.com
Visit www.symphonyai.com/eu-amla

About SymphonyAI

SymphonyAI, 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 2000 leading enterprises as clients globally. Since its founding in 2017, SymphonyAI has grown rapidly to 3,000 talented leaders, data scientists, and other professionals. SymphonyAI is an 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 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

© 2026 SymphonyAI. All rights reserved.