RSM

From compliance to competitive advantage

Rethinking **Anti Money Laundering** for crypto: navigating risk, regulation, and innovation in digital assets

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

Anti Money Laundering in crypto

Over the past five years, the digital asset market has surged from niche adoption to mainstream finance, with global crypto market capitalisation now exceeding $3 trillion. Decentralised finance (DeFi) protocols now handle billions in daily transactions, offering lending, staking, and liquidity services without intermediaries.

This rapid evolution brings unprecedented opportunities, alongside heightened Anti Money Laundering (AML) and regulatory challenges. Global and regional regulators are tightening oversight of crypto activities, mandating identity verification and data sharing under the FATF Recommunication 16 - Wire Transfers (FATF Travel Rule). In the EU, frameworks such as AMLD6 (Sixth Anti-Money Laundering Directive) and the Markets in Crypto-Assets Regulation (MiCA) introduce significantly stricter compliance obligations for crypto-asset service providers, driving the need for robust and well-embedded AML controls.

Recent EU AML developments further raise the compliance bar. The EU's 2024 AML Package established a new Anti-Money Laundering Authority (AMLA), which will directly supervise selected high-risk financial institutions, including certain crypto firms. In parallel, the revised Transfer of Funds Regulation extends the Travel Rule fully to crypto transfers, requiring complete originator and beneficiary information for all transactions, regardless of value. Together, these measures aim to close regulatory gaps, strengthen cross-border supervision, and ensure consistent AML enforcement across EU Member States.

Crypto's pseudonymous nature and global reach make it particularly attractive for illicit activities, including laundering the proceeds of crime and circumventing sanctions. The rise of decentralised platforms and privacy-enhancing technologies further complicates detection and monitoring, creating material AML exposure for exchanges and financial institutions. Against this backdrop, strong AML frameworks are increasingly viewed as a marker of credibility and regulatory alignment, helping crypto firms build trust with regulators and customers alike. Such transparency is critical to attracting institutional investors seeking a secure and compliant entry point into digital assets.

Why AML matters in 2026

Landscape

Despite the promise of blockchain transparency, crypto remains a prime target for financial crime. Regulators are imposing tougher rules and penalties, while privacy tools and decentralised platforms create new blind spots. Strong AML controls are essential to maintain compliance, protect reputation, and enable institutional adoption.

Vulnerabilities

The decentralised nature of crypto creates unique AML challenges. Peer-to-peer transfers, privacy coins, and mixers obscure transaction trails, while cross-chain bridges and decentralised finance (DeFi) protocols introduce complex risk points. These factors make detecting illicit activity far harder than in traditional finance.

Reputation

Failure to meet AML obligations can lead to severe regulatory penalties and loss of licenses, but the reputational damage is often greater. Crypto firms associated with illicit activity risk losing customer trust, investor confidence, and strategic partnerships threatening long-term viability.

In 2026, AML compliance remains a cornerstone of regulatory expectations for the digital asset sector. Robust AML controls are essential not only to meet legal obligations but also to protect firms from significant financial and reputational risk.

A clear example of this is the enforcement action taken by the **Central Bank of Ireland**, which in November 2025 imposed a **€21,464,734 fine on Coinbase Europe** for breaching its AML transaction monitoring obligations between April 2021 and March 2025.

As a virtual asset service provider, Coinbase Europe is required to monitor customer transactions on an ongoing basis. Where Coinbase Europe suspects that a transaction is facilitating money laundering or terrorist financing it is required to file a Suspicious Transaction Report (STR) with the national Financial Intelligence Unit (FIU) and Revenue Commissioners as soon as possible.

Coinbase Europe has been fined due to faults in the configuration of their transaction monitoring system, which resulted in more than 30 million transactions not being properly monitored over a 12-month period. The value of these transactions amounted to over €176 billion and accounted for approximately 31% of all Coinbase Europe transactions conducted in the period when the faults existed.

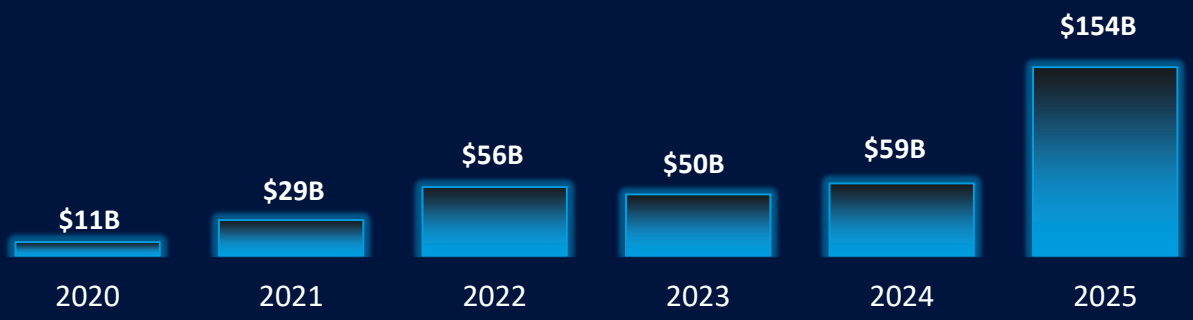
Further, it took Coinbase Europe almost three years to fully complete the monitoring of the impacted transactions. This subsequent monitoring led to the reporting of 2,708 STRs to the FIU for further analysis and potential investigation*.

Source: Central Bank of Ireland, November 2025

Is there money laundering in crypto transactions?

Although illicit activity on-chain previously revolved heavily around cybercrime, cryptocurrency is now also being used to fund and facilitate all kinds of threats, ranging from national security to consumer protection. As cryptocurrency has gained greater acceptance, illicit on-chain activity, too, has become more varied. For example, some illicit actors primarily operate off-chain, but move funds on-chain for laundering.

Total cryptocurrency value received by illicit addresses



Illicit cryptocurrency addresses received at least USD 154 billion in 2025. This represents a 162% increase year-over-year (YoY), primarily driven by a dramatic 694% increase in the value received by sanctioned entities. But even if the value received by sanctioned entities were flat YoY, 2025 would still mark a record year for crypto crime, as activity increased across most illicit categories.

Source: Chainalysis

How technology is reshaping AML compliance

One of the most transformative shifts in AML programmes is the rise of technology-driven compliance. Solutions like blockchain analytics, AI-powered transaction monitoring, and integrated compliance platforms are replacing manual reviews and fragmented processes. These tools enable real-time detection of suspicious activity, reduce false positives, and streamline reporting, making AML more proactive and efficient in the crypto space.

Real-world examples

Leading crypto firms that RSM works with, or observes across the market, leverage sophisticated blockchain analytics combined with AI-driven transaction monitoring to meet global AML and sanctions compliance requirements. These systems automatically flag high-risk wallet activity, screen transactions against sanctions lists, and support real-time risk assessment.

Other major digital asset platforms have implemented machine-learning-based KYC and transaction monitoring solutions, significantly reducing false positives and improving the identification of complex laundering typologies, including cross-chain movements and decentralised finance (DeFi) activity.

In addition, widely used AI-enabled compliance platforms in the crypto sector assist businesses in identifying high-risk wallets and meeting FATF Travel Rule obligations, offering continuous screening against global sanctions regimes and known suspicious activity indicators.

AML as a strategic risk management tool

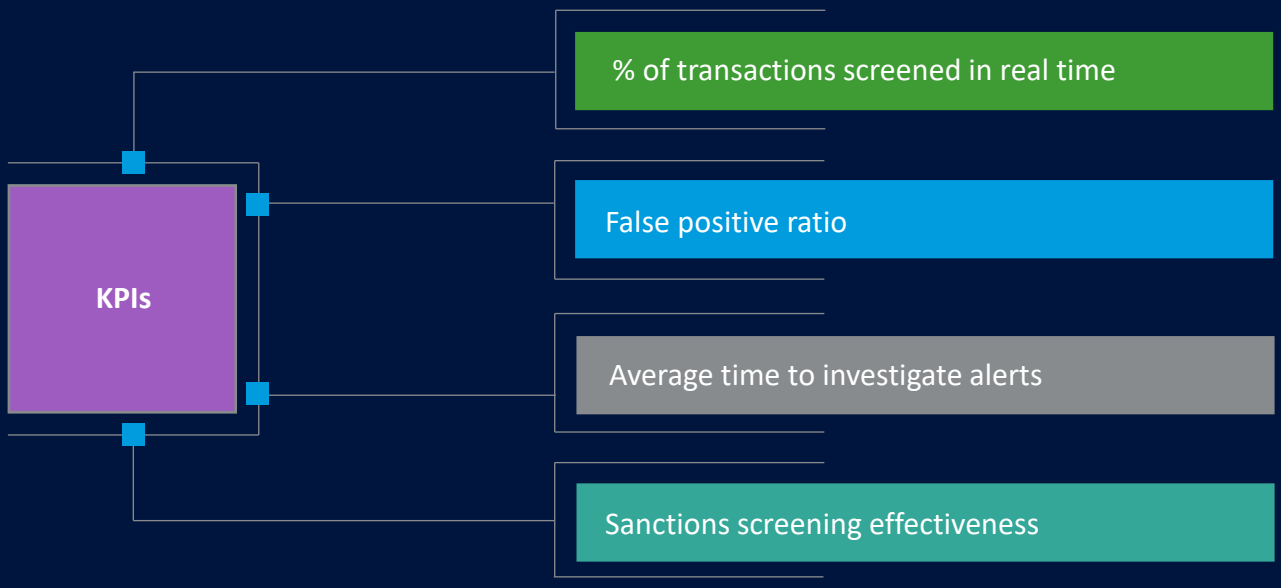
Beyond efficiency, a modern AML programme can serve as a strategic lens into enterprise risk. By integrating AML controls with broader risk management frameworks, crypto firms gain:

According to a top 10 global bank operating in Ireland, after deploying AI-driven AML tools, they now detect two to four times more financial crimes, reduce false positives by 60%, and cut review times from weeks to days. Additionally, according to Elliptic Research, 13% of all crypto transactions in DeFi protocols show exposure to high-risk wallets, increasing compliance complexity

- **Early warning systems** for suspicious wallet activity and high-risk transactions.
- **Cross-functional insights** into operational inefficiencies and compliance gap.
- **Improved alignment** between compliance, finance, and technology teams.
- **Enhanced resilience** against regulatory, reputational, and cyber risks.

The metrics that matter in crypto compliance

Supervisors increasingly look for data-driven evidence of AML effectiveness, particularly in higher-risk sectors like crypto. KPIs play a critical role in demonstrating control maturity, operational efficiency and ongoing compliance To measure AML maturity and effectiveness, track these KPIs:



AML programmes in the crypto space require clear metrics to demonstrate control health and compliance readiness. KPIs provide visibility into operational efficiency and risk exposure, enabling continuous improvement and regulatory confidence. By monitoring these indicators, firms can identify gaps early and strengthen their compliance posture.

Framework for a future-ready AML programme

To move from compliance to competitive advantage, crypto firms need a risk-based, technology-enabled AML framework. This means embedding automation, leveraging blockchain analytics, and aligning with global standards to ensure resilience and scalability. A future-ready AML programme should:

1	**Assess and map risks**	Identify high-risk assets, wallets, and transaction flows
2	**Enable real-time monitoring**	Deploy AI-driven tools for continuous screening
3	**Design and embed controls**	Integrate AML checks into onboarding, trading, and settlement processes
4	**Centralise evidence**	Use secure platforms for audit-ready documentation
5	**Test and validate**	Regularly review controls and explainable AI logic for regulatory trust
6	**Streamline walkthroughs**	Focus on changed or high-risk controls only
7	**Integrate with ESG and cyber**	Align AML with broader governance and sustainability goals

How RSM can help you elevate your AML programme

At RSM Ireland, we go beyond advising on AML - we work alongside you to help shape and strengthen your AML programme. Our team collaborates closely with your compliance and operations teams to design, implement, and review AML controls across crypto platforms. From transaction monitoring and blockchain analytics to regulatory reporting and technology enablement, we help make your programme efficient, resilient, and audit-ready - supporting you well before regulators or external reviewers step in.

Why RSM Ireland?

Global AML programme delivery

Through the RSM International network, we deliver AML programmes across Europe, North America, and APAC.

Smart compliance

We make use of trusted compliance platforms and blockchain analytics tools to help improve visibility, support timely insights, and enhance overall operational efficiency.

Audit-ready assurance

We act as your first line of defence, identifying and remediating control gaps before your external auditors do.

Custom risk-based compliance

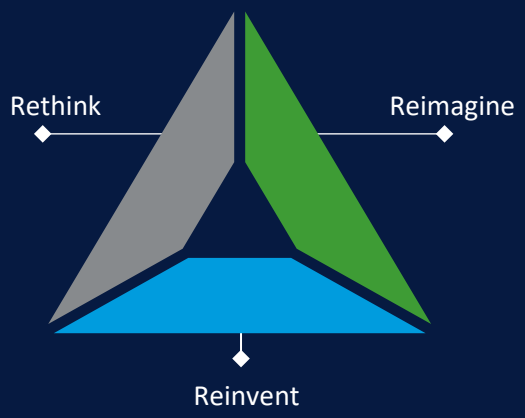
Our solutions are customised to your crypto business model, risk profile, and compliance maturity level.

Conclusion: Rethink, reimagine, reinvent

AML compliance is no longer about ticking boxes.

In 2026, it's about building a resilient, transparent, and technology-enabled compliance framework that safeguards trust and supports strategic growth. Modern AML programmes in the crypto space must go beyond regulatory minimums, leveraging automation, blockchain analytics, and AI-driven monitoring to deliver real-time risk insights and operational efficiency.

By rethinking your AML programme through the lens of automation, integration, and value creation, and with RSM Ireland as your partner you can turn a regulatory requirement into a competitive differentiator.



Next step

Contact RSM Ireland to assess your AML maturity and explore technology-driven compliance opportunities that deliver measurable value.

Colm is a Partner leading RSM Risk and Governance department. He has over 17 years of Risk and Governance experience and has established a market leading reputation for supporting Boards and Executive Management teams with their Risk and Governance practices.

Prior to joining RSM Ireland, Colm was senior assurance professional working out of London, Dublin and the US.

Colm is a Chartered Accountant and also holds the CFA, CIA and CISA designations.

Colm Laird
Partner
Colm.laird@rsmireland.ie

The RSM team:

Colm Laird

Partner, Risk and Governance
colm.laird@rsmireland.ie

Michael Mulholland

Partner, Head of Audit
mmulholland@rsmireland.ie

Paul Torres

Global Blockchain Director
paul.torres@rsmus.com

Drishti Rana

Director, Audit
drana@rsmireland.ie

Divan Steyn

Senior Manager, Risk and Governance
divan.steyn@rsmireland.ie

Ann Marie Conroy

Senior Manager, Risk and Governance
annmarie.conroy@rsmireland.ie

Sive Riznyczok

Manager, Risk and Governance
sive.riznyczok@rsmireland.ie

Yevgen Shuvalov

Consultant, Risk and Governance
yshuvalov@rsmireland.ie

THE POWER OF UNDERSTANDING
ASSURANCE | TAX | CONSULTING

RSM

RSM Ireland

Block D
Iveagh Court
Harcourt Road
Dublin 2
D02 VH94
Ireland
T +353 (0)1 496 5388
www.rsmireland.ie