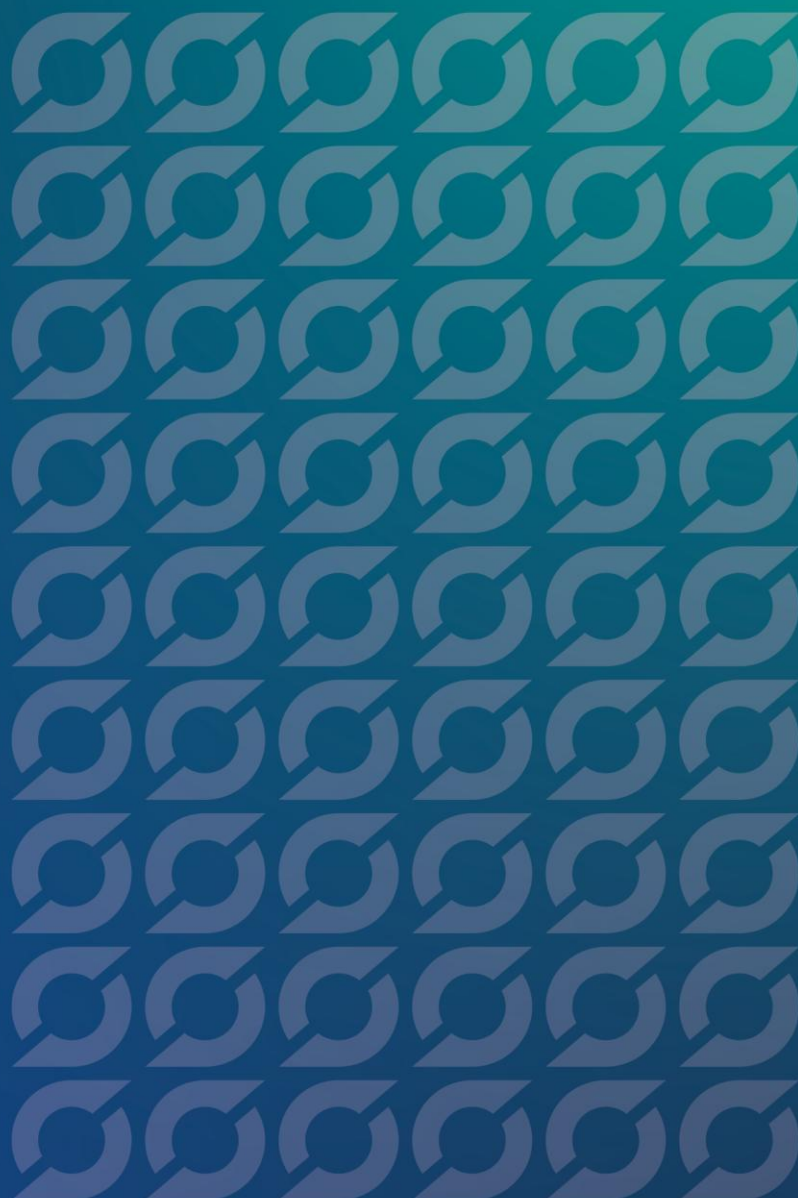


AMLA Roadshow

2025



Contents

1 Executive summary	4
1.1 Purpose of the Roadshow	4
1.2 Key insights at a glance	5
2 Introduction: twenty-seven countries, one conversation	7
2.1 A new authority, a first objective	7
2.2 Stakeholders met	7
3 Overview of cross-cutting themes	9
4 How risks were discussed with AMLA	12
4.1 Fraud	13
4.2 Crypto assets and services	13
4.3 Cross-border transactions and instant payments	14
4.4 Cash and real estate	15
4.5 Online and illegal gambling	16
4.6 Impact of geopolitical shifts	16
5 The challenges Europe is encountering	18
5.1 Legacy challenges: the weight of different starting points	18
5.1.1 Fragmentation of the supervisory and intelligence landscape	18
5.1.2 Low AML/cft maturity in the non-financial sector	19
5.1.3 Resource constraints across all sectors	20
5.2 Emerging challenges: technology and the pace of change	21
5.2.1 Technology gaps and digitalisation	21
5.3 Challenges in navigating regulatory complexity and change	22
5.3.1 Regulatory complexity, legal tension, and implementation pressure	22
5.4 What the challenges reveal	23
6 From findings to action: opportunities and AMLA's early response	24
6.1 The structural change of the EU's AML system: building a level playing field	24
6.2 New avenues for cooperation, coordination and support	27
6.2.1 Public-private partnerships and information sharing	27

6.2.2	Technology and shared infrastructure	28
6.2.3	Capacity building	29
6.3	The work ahead	30

Foreword by Bruna Szego, Chair of AMLA

When I took up my duties as Chair of AMLA in February 2025, I set myself an objective to visit **all 27 EU Member States** and meet the people on whose work **Europe’s fight against money laundering and terrorist financing** depends. National supervisors, financial intelligence units (FIUs), financial institutions, insurers, crypto-asset service providers, accountants, lawyers and notaries, real estate agents, and many others—the full range of public and private-sector actors who together form **the backbone of the system AMLA is here to strengthen**.

By December 2025, that objective was met.

This report is the result of those conversations. Over the course of the year, my colleagues and I sat in **roundtables across every corner of the Union**—from Lisbon to Helsinki, from Nicosia to Dublin—and we listened. We heard about **the pressures supervisors face** as the risk landscape shifts faster than their resources allow. We heard from **FIUs managing rising volumes of suspicious activity reports** with tools that have not always kept pace with the threat. We heard from businesses—large and small, financial and non-financial—about the complexity of **a system that varies significantly from one Member State to the next**, and about their genuine wish to do their part.

What struck me most was not the diversity of national contexts—which is real and significant—but **the degree of shared experience** across them. The same concerns surfaced in country after country: **fragmentation, resource pressure, the challenge of keeping pace with rapidly evolving risks**, and a strong desire for the kind of EU-level coordination that AMLA will provide. **Technology** ran through almost every conversation—as a source of new risk, and as **the most promising lever for making supervision more effective**.

We are publishing this report because we believe the conversations we had belong to everyone who participated in them. The people and organisations who gave their time and spoke openly deserve to see what we took away. And the broader public has an interest in understanding **the state of Europe’s defences against financial crime**—and **what is being done to strengthen them**.

We are carrying these insights into **AMLA’s work**—into **the standards we set, the guidance we provide**, and the way we engage with supervisors, FIUs, and the private sector going forward. **The Roadshow was a beginning, not a conclusion**.

I am grateful to everyone who participated. Your candour made this exercise worthwhile.

Bruna Szego Chair, Anti-Money Laundering Authority Frankfurt, 2026

1 Executive summary

1.1 Purpose of the Roadshow

Money laundering and terrorist financing pose a **serious threat to the EU’s security and the integrity of the internal market**. Money laundering—the process by which illicit proceeds are made to appear legitimate—costs European society **billions of euros** every year. It funds organised crime, fuels corruption, and distorts fair competition. Terrorist financing, while often involving smaller sums, is nonetheless critical as it enables terrorist actors and networks to plan, sustain and execute attacks. These phenomena are increasingly **cross-border in nature**: criminal and terrorist networks operate **transnationally**, and illicit funds can be moved rapidly across jurisdictions, exploiting **gaps and inconsistencies**. Tackling money laundering and terrorist financing therefore requires not only strong action at national level, but also **a coordinated response at EU level** that supports effective cooperation and timely information exchange across borders.

The **Anti-Money Laundering Authority (AMLA)** is the European Union’s new agency established to lead that response. Created by EU legislation and headquartered in Frankfurt, AMLA began operations in 2025. AMLA was set up to address **long-standing fragmentation** under the previous directive-based model and to strengthen the consistent application of **anti-money laundering and countering the financing of terrorism (AML/CFT) requirements** across the Union through a **more harmonised framework**. Its role is to set **common standards** for how financial and other institutions across all 27 Member States prevent and detect money laundering and terrorist financing, **promote supervisory convergence**, and **strengthen cooperation among national supervisors and FIUs**. In addition, AMLA will directly supervise a limited number of the most impactful financial institutions or groups operating across borders.

It is clear that AMLA can only succeed if it understands **the realities on the ground**—the challenges facing those who supervise obliged entities, the concerns of businesses navigating new rules, and the expectations of all those with a stake in a cleaner, safer financial system. This report is the result of that commitment: **to listen before acting**.

Between March and December 2025, AMLA’s Chair, Bruna Szego, conducted a Roadshow covering **all 27 EU Member States**. In each country, she met **national supervisory authorities, FIUs, and representatives from the private sector**—banks, insurers, crypto-asset service providers (CASPs), accountants, lawyers, notaries, real estate agents, and many others. In total, the Roadshow brought together **hundreds of organisations and individuals across Europe**. All discussions were held under the **Chatham House Rule**, and the expressed views are presented here in aggregated form without attribution.

This report is an **honest reflection on the state of AML/CFT efforts across Europe**: where the system is working, where it is falling short, and what AMLA, national supervisors, FIUs, and the private sector can each do to contribute to a **better functioning AML/CFT system in the EU**.

1.2 Key insights at a glance

Despite the diversity of national systems, supervisory traditions, and economic contexts across the EU, the Roadshow revealed **a striking degree of shared experience. Five themes emerged consistently across all 27 Member States.**

First, the **money laundering and terrorist financing (ML/TF) risk landscape is shifting fast.** Long-standing typologies have not disappeared, but they are now increasingly accompanied by faster-moving developments driven by **technological innovation and geopolitical dynamics.** Risk perceptions were also shaped by geography, with Member States' priorities reflecting differing exposures, cross-border interconnections, and regional transmission channels.

Second, **Member States and sectors are starting from materially different baselines.** Stakeholders described uneven supervisory practices, enforcement cultures, analytical tools, and levels of maturity across the Union, which can translate into **inconsistent implementation** and create **vulnerabilities** that criminals may exploit across borders. While progress is visible in some areas, the Roadshow feedback repeatedly highlighted that parts of the **non-financial sector lagged behind the financial sector** in terms of AML/CFT awareness and capability, often reflecting limited resources and fragmented supervisory arrangements.

Third, **technology is both a risk driver and a solution enabler.** Technological developments can accelerate threat typologies and compress detection windows, creating **new operational challenges** for both obliged entities and supervisors. At the same time, they offer significant opportunities to **enhance risk detection, strengthen supervisory effectiveness** and **reduce unnecessary compliance burden.** Stakeholders highlighted the potential in **advanced data analytics, interoperability and shared tools** in particular—especially if the new EU architecture can reduce redundancy and support common, scalable solutions where appropriate.

Fourth, **the reform of Europe's AML/CFT system is broadly welcomed.** The new EU framework—including a **directly applicable Single Rulebook** and the establishment of AMLA—was seen as a turning point to address the long-standing fragmentation associated with the previous directive-based model and to **support more consistent supervision across the Union.** Stakeholders also highlighted the opportunity for a more harmonised framework to simplify compliance over time by **reducing inconsistencies** across Member States and **limiting unnecessary duplication**—such as overlapping information requests or divergent reporting formats for cross-border groups—thereby establishing a **level playing field.**

Fifth, **expectations towards AMLA are high and often very specific**, ranging from guidance on emerging risks and the simplification of rules to the development of shared supervisory tools and stronger cooperation mechanisms. The message across Europe was broadly consistent: **AMLA has a unique opportunity to contribute to a better-functioning AML/CFT system**, but only if it remains closely connected to **operational realities**. At the same time, stakeholders' expectations will need to be **calibrated against actual constraints**. AMLA's mandate conferred by the AMLA Regulation clearly delineates the scope of its action and the instruments at its disposal. In many cases, the suggestions made related to changes that would require amendments to the legislative framework at Level 1 and therefore **fall outside AMLA's remit**. Similarly, expectations on speed and breadth of IT systems and tools to be developed by AMLA exceed what can be delivered in the short term, as the focus, for now, lies in **building the core infrastructure**. Finally, some expectations directed at AMLA should be more appropriately addressed to national competent authorities, as AMLA is not empowered to address them. For example, while AMLA can support supervisory convergence and coordination at Union level, **capacity-building and direct engagement with obliged entities will remain primarily the responsibility of national supervisors**.

We take these findings seriously. The chapters that follow set out the detail behind each of these themes. They are **the foundation for the work AMLA is now undertaking** to strengthen Europe's defences against financial crime in close partnership with national supervisors, FIUs, and private-sector actors we met along the way.

2 Introduction: twenty-seven countries, one conversation

AMLA's initial focus includes **building effective working relationships** across the EU AML/CFT ecosystem. In 2025, Chair Bruna Szego **visited all 27 Member States** to meet **national supervisors, FIUs, and private-sector representatives**—sharing AMLA's vision and learning from theirs. This report distils the main insights from those conversations and provides **a comprehensive picture of the state of AML/CFT efforts across the European Union.**

2.1 A new authority, a first objective

As a **newly established EU authority**, AMLA is developing an engagement approach commensurate with its broad mandate and Union-wide reach. Following her appointment in February 2025, Chair Bruna Szego met all members of the **AMLA General Board**, which comprises representatives from the AML/CFT supervisory authorities and FIUs from all EU Member States. The Roadshow formed part of this early effort to **build mutual understanding**, establish channels for cooperation and ensure that **AMLA's priorities remain grounded in operational realities across jurisdictions and sectors.**

2.2 Stakeholders met

Each visit during the Roadshow included a **public-sector roundtable** hosted by the national supervisory authorities, bringing together the relevant authorities involved in **AML/CFT supervision and financial intelligence** at national level.

These public-sector sessions were complemented by **private-sector roundtables in 24 out of 27 Member States**. Due to logistical constraints, the first three stops could not accommodate private-sector meetings, but all subsequent visits included them. The sessions were organised at sector level and therefore primarily involved **industry associations rather than individual firms.**

Across Member States, private-sector participation covered a **broad range of obliged entities**, including representatives from the banking, insurance, and securities sectors, payments and e-money, crypto-asset service providers, as well as real estate, gambling, lawyers, notaries, accountants and high-value goods traders. This ensured that both the **financial and non-financial sectors** were represented. Participation levels varied by country, reflecting differences in national supervisory arrangements, the structure and maturity of sectoral representation, and the way responsibilities are distributed across authorities and professional bodies. Despite these

variations, every roundtable offered a **rich and comprehensive view of national supervisory landscapes and industry expectations across the EU.**

Across the Roadshow, the Chair returned consistently to **three messages** that she regards as central to understanding both AMLA's mandate and the moment it finds itself in. AMLA was established with **a dual purpose**: to **address failures** that had accumulated under the EU's previous AML/CFT architecture, and to build a framework capable of responding to a risk environment that is **structurally more demanding** than the one the old system was designed for. Delivering on that purpose, she emphasised, depends fundamentally on **cooperation**—with national authorities, FIUs and the private sector alike. This is not an operational preference but a **design principle of the new framework**. Finally, the scale of change brought by the legislative package is significant, and **preparedness cannot be assumed**. The Chair was particularly direct on this point in relation to the non-financial sector: awareness among both supervisors and obliged entities of what the new framework will require remains uneven, and **raising that awareness at national level is a priority** that cannot wait for the framework to be fully in place.

3 Overview of cross-cutting themes

Each session followed a consistent format: the Chair opened with a framing principle—that **AMLA’s effectiveness depends on sustained collaboration** with national supervisors, FIUs, and the private sector—before guiding participants through a common set of questions covering the **main challenges, opportunities, and implementation issues** arising from the new EU AML/CFT framework. Participants were also invited to raise emerging risks, sector-specific concerns, national priorities, and any other issues they considered relevant.

All discussions were held under the **Chatham House Rule**, enabling an **open and candid exchange**. Individual contributions are therefore not attributed to specific institutions or authorities, but are reflected here in **aggregated form**, focusing on **common trends and recurring themes** that emerged consistently across Member States.

The Roadshow revealed **a high degree of commonality in stakeholder perspectives**, notwithstanding differences in supervisory structures, sectoral composition, and levels of institutional maturity and capacity. The analysis focused on **three core questions**: (i) which ML/TF risks stakeholders consider most important, (ii) which challenges they regard as most pressing, and (iii) which opportunities they see for improving the effectiveness of AML/CFT action at both national and Union level. On this basis, **five themes emerged consistently** from discussions with national supervisors, FIUs, industry associations and professional bodies.

First, stakeholders across both the public and private sectors underlined a **rapidly evolving ML/TF risk landscape**. New threat vectors and vulnerability drivers are increasingly shaped by **technological developments and geopolitical shifts**, although different elements of that landscape were emphasised more strongly by different stakeholder groups. Financial-sector participants, particularly from the private sector, highlighted the growing relevance of **fraud and scam typologies**, including AI-enabled impersonation, as well as **the speed and reduced intervention window associated with instant payments**. Risks linked to the expanding use of **crypto-assets and related services** were raised mainly by public-sector authorities within the financial sector. **Sanctions-related risks and circumvention concerns** were emphasised most prominently by stakeholders in Member States with heightened geopolitical exposure. At the same time, stakeholders—primarily in the non-financial sector—observed that **long-standing enablers of money laundering**, including cash-intensive businesses and the misuse of legal persons and business structures, remain highly relevant.

Second, stakeholders emphasised that **Member States and sectors are starting from materially different baselines**. In the public sector, they pointed to **fragmentation in supervisory practices and uneven FIU capabilities** across the EU. These disparities were seen as particularly pronounced in the non-financial sector, especially because of the multiplicity of competent

authorities involved, which contributes to a highly heterogeneous supervisory landscape. Stakeholders also highlighted that, compared to the financial sector, **AML/CFT maturity in the non-financial sector remains generally lower**, with many obliged entities still having **limited awareness** of their obligations and, in some cases, **insufficient capacity** to conduct checks in a robust and consistent manner. Those weaknesses are often compounded by **resource constraints**, incomplete visibility of the obliged-entity population in certain sub-sectors and limited supervisory reach. Private-sector representatives echoed many of these concerns, pointing to uneven application of rules across Member States, **divergent supervisory expectations**, and resulting **compliance complexity**—especially for cross-border groups.

Third, **technology was consistently framed as both a driver of risk and an enabler of solutions**. Stakeholders highlighted that digital innovation is accelerating and reshaping the ML/TF risk landscape, while also increasing **operational pressures** for both obliged entities and competent authorities. At the same time, the Roadshow underlined that technology can materially **strengthen the effectiveness of the AML/CFT system**. **Advanced analytics, AI-supported tools, interoperable data infrastructures, and greater automation** were widely seen as capable of supporting faster identification of emerging patterns, more targeted supervision, and reduced duplication in compliance processes. In this context, stakeholders underlined the importance of strengthening **Union-level analytical capacity** and, over time, developing **shared tools**.

Fourth, across the board, the **EU AML/CFT reform was seen as a major opportunity** to move away from the limitations of the previous directive-based framework, under which differences in transposition and supervisory practice contributed to fragmentation. Supervisory authorities and FIUs highlighted the added value of **the Single Rulebook** in strengthening legal certainty and consistency, alongside **enhanced cooperation mechanisms, stronger supervisory convergence** and a more uniform application of the **risk-based approach** to AML/CFT supervision. Private-sector representatives likewise welcomed the prospect of a **more predictable and efficient framework**, in which obligations are applied more consistently across Member States, unnecessary duplication for cross-border groups is reduced, and compliance is less likely to become a competitive disadvantage.

These four themes translate directly into the fifth: **expectations towards AMLA**. Stakeholders consistently saw AMLA as well placed to contribute to **a more coherent understanding of emerging ML/TF risks** relevant to the internal market and to foster awareness and responsiveness to those risks across supervisors and FIUs. AMLA was also seen as having a **central role in promoting supervisory convergence**, facilitating the **diffusion of best practices** and supporting the **development of a common supervisory culture** across the Union, while contributing to stronger coordination and a **more even baseline of analytical and operational capacity among FIUs**. Stakeholders also saw AMLA as capable of adding value by **supporting national authorities in less mature sectors**, promoting more consistent approaches to the use of technology, and providing guidance on information-sharing challenges.

At the same time, **expectations need to remain realistic**. Capacity-building and day-to-day support for obliged entities will remain primarily **the responsibility of national authorities**, while AMLA's most immediate contribution is more likely to come through **convergence tools, guidance, training and cooperation frameworks** directed at national supervisors and FIUs. Likewise, although many stakeholders stressed the importance of **proportionality and simplification** when completing the Single Rulebook through Level 2 and Level 3 instruments, these must operate within **the boundaries set by the Level 1 legislation**.

4 How risks were discussed with AMLA

Across all 27 Member States, the Roadshow revealed similarities in how supervisors, FIUs, and private-sector stakeholders characterise the ML/TF risk landscape, notwithstanding the diversity of national contexts. **Two findings carry particular analytical weight.** First, stakeholders consistently described a **rapidly evolving environment**, in which both threat typologies and vulnerabilities are changing quickly, driven above all by **technological developments** and, increasingly, by **geopolitical dynamics**. Secondly, the most urgent expectations directed at AMLA are centred on **emerging risks**, rather than on long-standing ones that national systems have more experience managing. This distinction underpins the analysis in this chapter and informs how AMLA's expected value-added is framed.

Throughout the Roadshow, national authorities highlighted a combination of prominent threat areas, vulnerabilities in products, services and sectors that may be exploited, and contextual factors that can amplify exposure, such as geopolitical tensions. A common thread across these categories was the operational premium placed on **timely detection and cross-border coordination** as criminal methods adapt to digitalisation and technological innovation.

At the same time, the Roadshow also showed that **risk perception and prioritisation** are shaped by geographic placement and resulting exposures. In Member States with heightened proximity to geopolitical tensions, **sanctions-related risks and evasion typologies** were more frequently emphasised as supervisory priorities, consistent with the growing salience of targeted financial sanctions and related evasion concerns in the EU policy and supervisory context. In other jurisdictions, stakeholders attached particular significance to vulnerabilities linked to national economic features and sectoral concentration—for example, risks associated with **real estate transactions or gambling** where these activities are especially prominent—illustrating that common EU-wide trends are filtered through **distinct local exposure profiles**.

Long-standing risks remain material across the Union. Stakeholders noted that persistent vulnerabilities—such as cash-intensive activity, real estate-related exposures, and the misuse of legal persons and corporate structures—continue to interact with established threats, including drug trafficking and other proceeds-generating offences. These high-risk areas are widely recognised.

Emerging risks tell a different story. Several emerging threats—notably **technology-enabled fraud** (including deepfakes) and **sanctions-evasion typologies**—were repeatedly highlighted alongside accelerating vulnerability drivers, such as the speed and irrevocability of instant payments, increased reliance on remote onboarding and digital identity solutions, and the growing use of

crypto-asset products and services. Stakeholders emphasised that **AMLA's comparative advantage lies in supporting and coordinating a more coherent, cross-border response** where fast-evolving threats exploit vulnerabilities that are shared across jurisdictions and sectors—consistent with AMLA's role in **promoting convergence and effective cooperation** across the EU AML/CFT system.

4.1 Fraud

Fraud was identified as **one of the most significant and fastest-growing areas of criminal activity**. Stakeholders, especially from the private sector, noted that **the boundary between fraud and money laundering is increasingly blurred**, as illicit proceeds generated through fraud can rapidly enter laundering channels, requiring controls that address both predicate conduct and subsequent laundering behaviour. Some industry associations reported that a limited number of financial institutions are responding by **consolidating fraud and AML functions** within the same departments to reflect these connected risk pathways.

Technology was highlighted as a consistent driver: the use of **AI-generated synthetic media** (including deepfakes) enables **impersonation and identity fraud at scale**, the expansion of remote onboarding creates an additional vector for **identity abuse**, and the availability of **instant payments** compresses ex-ante intervention timeframes and increases reliance on effective, real-time controls (see Section 4.3).

While **AMLA does not directly combat fraud**, its mandate intersects with **fraud-related risks** due to their close link with money laundering activities. Fraud is becoming increasingly significant as a **predicate offence**. To fight it efficiently, **a comprehensive approach** is needed, one that takes into account both the financial and other sectors. Within the financial sector this means coordinating the upcoming third Payment Services Directive (PSD3) and Payment Services Regulation (PSR) requirements with AML/CFT requirements to avoid duplication. It also means taking other sectors such as telecommunications and internet services and social media platforms into account. These must be considered to **prevent fraud at source** as they can be exploited to facilitate fraudulent activities.

4.2 Crypto assets and services

ML/TF risks linked to crypto assets and related services were raised across a large majority of Member States. Stakeholders noted that, as the EU crypto-asset framework under the **Markets in**

Crypto-Assets Regulation (MiCA) moves from rule-setting into implementation through sustained authorisation and **supervision of CASPs**, material supervisory and operational challenges remain, including the need to ensure **consistent supervisory approaches across jurisdictions**.

Stakeholders also pointed to structural vulnerabilities, including the **limited transparency around counterparties and beneficial ownership**, the **cross-border nature and speed of crypto-asset transfers**, and uneven levels of supervisory experience and resourcing across competent authorities. They also reported **reliance on specialist blockchain analytics** and other external tools to support monitoring and investigations, noting that costs can be significant as capability is concentrated among a limited set of providers.

The speed of crypto-asset transfers and products with identity-obscuring features have previously been identified as factors that can increase ML/TF risk. These concerns also align with AMLA's early public messaging and work programme, which identify the crypto sector as a **high-risk area** and an early priority for promoting high AML/CFT standards and supervisory convergence across the Union.

In that context, stakeholders expected AMLA to lead on **harmonised CASP supervision standards**, contribute to a **common understanding of crypto-related typologies and vulnerabilities**, strengthen **EU-based analytical capabilities and common infrastructures** where possible, and facilitate cooperation and information exchange, in line with its broader mandate to promote consistent and effective AML/CFT supervision and coordination across the Union.

The non-financial sector was generally perceived as having comparatively lower direct exposure to crypto assets and crypto-related risks, although this may vary by Member State.

4.3 Cross-border transactions and instant payments

Cross-border ML/TF risk is both persistent and, in some areas, accelerating. Stakeholders emphasised that the wider availability of **instant payments** introduces an additional operational challenge: funds can now move across borders in **near real time, 24 hours a day**, fundamentally **shortening the time available to identify and act on risk signals**, increasing the importance of timely monitoring, effective safeguards and rapid information exchange.

In this context, control arrangements that rely primarily on **end-of-day batch processing and next-day review are less well suited** to detecting and interrupting fast-moving typologies. This creates pressures not only for obliged entities, but also for supervisors and FIUs, particularly in cross-border contexts where detection and response often depend on **timely cooperation and information sharing across jurisdictions**—an issue that EU legislation increasingly seeks to address through stronger coordination mechanisms.

The **EU Instant Payments Regulation** is intended to accelerate the roll-out of instant credit transfers within the Union, reinforcing the importance of ensuring that AML/CFT frameworks and operational processes remain effective in a **faster, more continuous payments environment**.

4.4 Cash and real estate

Cash remains a material ML/TF risk factor across multiple sectors, and its persistence alongside the ongoing digitalisation of finance underlines that **cash-based laundering has not been displaced**; rather it continues to coexist with emerging digital typologies.

The **real estate sector** likewise continues to present **significant money laundering potential**. This reflects both the size of the market and its ability to absorb large amounts of funds in a secure and stable environment while offering economic returns. These features are compounded by the widespread opportunities for **obfuscation of true beneficial ownership** through nominees or opaque legal structures, as well as by the **opacity of asset valuation**.

Exposure and risk are not uniform across Member States or across segments of the real estate market. Stakeholder feedback suggests that **higher ML risk** tends to arise in local markets characterised by a stronger investment real-estate profile, higher-value transactions, ready access to liquidity, differing roles and profiles involved in transactions, and greater cross-border participation in property acquisitions or ownership arrangements. The presence of **notaries** involved in transactions—which is not required everywhere in Europe—was generally seen as a mitigating factor.

Stakeholders also pointed to **significant heterogeneity in terms of AML/CFT maturity** across the sector, including across Member States and among the intermediaries involved in real estate transactions. They highlighted **uneven levels of AML awareness and operational capacity**, with some intermediaries demonstrating limited familiarity with customer due diligence and suspicious transaction reporting obligations.

In this context, the Roadshow feedback suggests that AMLA could add value by **promoting common, high-quality supervisory approaches and by fostering capacity-building** among national supervisors in their respective sectors, especially where supervisory maturity is still developing. This would contribute to **more consistent and effective supervision** across the Union, while primary responsibility for awareness-raising and compliance at the level of obliged entities remains with national authorities.

4.5 Online and illegal gambling

While cash intensity in traditional gambling remains a well-established ML/TF risk, **online and illegal gambling** emerged across the Roadshow as an increasingly pressing concern. Supervisors and FIUs pointed to **online gambling platforms operating outside EU jurisdictions** as a growing ML/TF vector, combining the speed and, in some cases, anonymity of digital payments with **limited supervisory reach**.

In parallel, private-sector participants highlighted that the **absence of harmonised rules across Member States** constitutes a **structural vulnerability**, resulting in fragmented and sometimes overlapping national regimes. This fragmentation was seen as creating scope for both **regulatory arbitrage** and uneven competitive conditions for licensed operators. This is an area where stakeholders explicitly identified **EU-level harmonisation** and **AMLA's coordination role** as having direct practical value.

4.6 Impact of geopolitical shifts

Sanctions circumvention has become a more prominent supervisory and enforcement concern since 2022, against the backdrop of Russia's full-scale invasion of Ukraine and the resulting intensification of the EU sanctions regime. Roadshow feedback suggests that this has been particularly salient in Member States with **heightened geopolitical exposure**, including in parts of the Baltic, Nordic, and Eastern European regions, where **sanctions-related risks** have increasingly influenced supervisory priorities and compliance resourcing.

More broadly, stakeholders pointed to a risk environment driven by **geopolitical dynamics** that has become more complex and fast-moving, marked not only by increasingly sophisticated sanctions-evasion techniques, but also by the interaction of sanctions risks with wider threats, including **cyber-enabled criminal activity**. This assessment is consistent with EU-level threat analyses, which point to a sustained increase in cyber-enabled activity since 2022, including **ransomware and availability attacks**, often linked to or facilitated by geopolitical tensions.

Participants also highlighted an **uneven capacity to manage these pressures** across sectors. Large financial institutions were generally described as having invested significantly in AML/CFT compliance infrastructure, whereas parts of the **non-financial sector** reported **more limited resources** and, in some cases, **lower awareness** of the scope of sanctions-related obligations. Stakeholders suggested that such a capacity gap can create **vulnerabilities** that may be exploited in circumvention schemes, particularly where controls are less mature.

In addition, some stakeholders referred to the persistence of **international terrorism** as a background risk factor in the current geopolitical environment. EU threat assessments continue to underline that terrorist financing risks remain present and adaptive, increasingly intersecting with cross-border payment channels, online platforms and, in some cases, the misuse of digital assets—reinforcing the need for **timely information-sharing and coordinated analysis**.

In this context, stakeholders pointed to the value of **EU-level aggregation of typologies and risk indicators**, and of **more structured cross-border coordination**, to support consistent identification of patterns and vulnerabilities in fast-evolving, geopolitically driven risk areas—with AMLA playing **a leading role that no national authority could replicate alone**.

5 The challenges Europe is encountering

While the previous pages outlined *what* established phenomena and emerging risks stakeholders are facing, this chapter examines *why responding effectively remains difficult*. Despite differences in national contexts, discussions with supervisors, FIUs, and private-sector actors across the EU identified **a broadly common set of challenges**. The recurrence of the same issues across all 27 Member States suggests that the obstacles to effective AML/CFT implementation are not primarily country-specific, but **structural in nature**.

Three challenge categories emerged from the Roadshow. First, **legacy challenges** reflect accumulated fragmentation and capacity gaps that developed under the pre-reform framework and continue to shape the conditions in which the new package must be implemented. Second, **emerging challenges** are generated—or intensified—by the same technological developments and geopolitical shifts described above. In other words, the factors reshaping ML/TF threats, vulnerabilities and risks are simultaneously creating **new challenges for effective supervision and risk management**. Third, stakeholders pointed to challenges in navigating **regulatory complexity and change**, particularly in balancing AML/CFT obligations with General Data Protection Regulation (GDPR) requirements and in addressing concerns about the timing of AMLA’s delivery of Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS).

Across all categories, a central tension was repeatedly emphasised: **the demands placed on the system are growing faster than its capacity to respond**.

5.1 Legacy challenges: the weight of different starting points

5.1.1 FRAGMENTATION OF THE SUPERVISORY AND INTELLIGENCE LANDSCAPE

The most pervasive legacy challenge identified across the Roadshow is **fragmentation**, which is rooted in the previous AML/CFT framework’s reliance on **national transposition and implementation**. In practice, fragmentation in AML/CFT supervision manifests and operates at multiple levels, *inter alia*, in **divergent supervisory methodologies**, risk assessment approaches, enforcement practices, and interpretations of AML/CFT requirements. Across Member States, supervisors apply materially different approaches to comparable risks, resulting in **inconsistent supervisory expectations** for obliged entities operating across borders and, in some cases, opening space for **jurisdiction shopping**. Within Member States, fragmentation is particularly evident in parts of the non-financial sector, where supervisory responsibilities are often spread

across **multiple bodies with overlapping or unclear mandates**, increasing coordination costs and contributing to **uneven supervisory outcomes** (see Section 5.1.2).

These divergences are compounded by challenges in **cross-border cooperation and information exchange**. Stakeholders noted that, while cooperation mechanisms exist, coordination and information flows are not always sufficiently timely, structured or consistent—particularly in the contexts where it matters most, such as the supervision of cross-border groups.

FIUs described a related, but distinct, dimension of the same problem. Differences in **analytical capabilities, resourcing and information-sharing practices** across jurisdictions can affect the consistency and usability of financial intelligence and the speed and quality of cross-border cooperation.

As a result, the EU AML/CFT system has been perceived as **formally interconnected, yet operationally uneven**—precisely the type of fragmentation that the 2024 reform seeks to reduce through a more harmonised corpus of rules, stronger cooperation between relevant authorities and a more consistent, risk-based supervisory approach across the Union.

5.1.2 LOW AML/CFT MATURITY IN THE NON-FINANCIAL SECTOR

A recurring finding across the Roadshow was the **comparatively lower level of AML/CFT maturity in the non-financial sector**. Stakeholders described this as manifesting in **two related ways**. First, many obliged entities—particularly smaller firms and sole practitioners in sectors such as real estate services, accountancy, notarial services, and the trade in high-value goods—were described as having **limited awareness of their AML/CFT obligations** and/or of how to execute them in practice. This extends beyond uncertainty in recognising red flags, making suspicious transaction reports where appropriate, and also reflects more practical constraints, including **limited access to relevant information** and a **lack of tools** needed to conduct meaningful customer due diligence and risk assessments.

Against the broader backdrop of capability and awareness constraints, some professional associations - particularly lawyers providing services under the EU AML/CFT framework - referred to legal privilege / professional secrecy as a potential limitation in applying AML/CFT requirements. AMLA notes that the EU legal framework already provides rules on that protection, which do not amount to a general exemption from AML/CFT requirements for the affected obliged entities.

Stakeholders further noted that supervisory responsibility in the non-financial sector is frequently dispersed across **multiple bodies**—supervisory authorities, FIUs, or self-regulatory bodies—with **differing mandates, powers, and levels of AML/CFT expertise**. The cumulative effect can be a **fragmented supervisory landscape** in which accountability is diffused, coordination costs are

high, and obliged entities are faced with inconsistent supervisory expectations depending on the authority responsible for their oversight. This heterogeneity was frequently cited as **a barrier to consistent and effective supervision** and to the development of a shared compliance culture across non-financial sub-sectors.

One observation from the Roadshow was particularly illustrative. Low volumes of suspicious transaction reporting from the non-financial sector were sometimes interpreted positively by practitioners—as evidence of limited risk exposure—whereas supervisors and FIUs consistently read the same pattern as an indicator of **systemic under-detection and under-reporting**. This divergence reflects **a structural awareness and capability gap** that is unlikely to be addressed through legal obligations alone.

5.1.3 RESOURCE CONSTRAINTS ACROSS ALL SECTORS

Almost every stakeholder group reported **a persistent mismatch between the resources available and the mandates** that competent authorities and obliged entities are expected to fulfil. These constraints were described as both **human and technological** in nature, although the results differ across the AML/CFT system.

In the public sector, financial supervisors frequently cited **limited access to specialist expertise** in rapidly evolving areas, notably crypto-asset products and services and other technology-enabled typologies. Non-financial supervisory authorities, on the other hand, often highlighted the structural challenge of delivering effective, risk-based oversight with **very small, dedicated AML/CFT units**, despite large and heterogeneous obliged-entity populations. FIUs similarly pointed to capacity pressures, describing **rising operational demands**—driven in part by increasing volumes of suspicious transaction reports and the broadening of responsibilities—**without commensurate growth in staffing or technological capability**.

In the private sector, financial institutions pointed to **escalating compliance costs** and the growing need for specialist expertise and sophisticated systems to manage faster-moving risks. In the non-financial sector, which is dominated by small firms and sole practitioners, AML/CFT compliance was often described as one of several regulatory obligations that collectively can **exceed available administrative capacity**.

Resource constraints are therefore not a peripheral issue; they constitute the operating condition within which every other challenge must be addressed.

5.2 Emerging challenges: technology and the pace of change

5.2.1 TECHNOLOGY GAPS AND DIGITALISATION

The Roadshow confirmed that **technological developments driving emerging ML/TF threats** are also generating **new implementation challenges**—and that the gap between what technology demands for effective supervision and compliance and what many competent authorities and obliged entities can currently deliver is widening.

In the public sector, supervisors reported recurring constraints in **procuring, operating and governing appropriate tools**, as well as in recruiting and retaining specialist profiles needed to maintain an adequate technological capability. FIUs highlighted persistent challenges related to **system interoperability and information exchange**, together with **insufficient automation and analytical capacity**, at a time when both suspicious transaction reporting volumes and case complexity are increasing.

As already highlighted earlier in this report, financial institutions in the private sector—which are generally better resourced—emphasised the growing pressure resulting from **the pace and sophistication of the evolving threat environment** and the technological adjustments required to respond effectively to new typologies. Furthermore, they noted that increased reliance **on remote onboarding and digital identity verification** can create vulnerabilities where **tools, data and control frameworks are not sufficiently robust**. In the non-financial sector, **the technological divide** was described as more **acute**: for many small obliged entities, digital and data-driven compliance solutions were seen as **too complex, costly or difficult to integrate** into day-to-day operations. Without accessible shared tools, clear operational guidance and, where appropriate, support mechanisms to facilitate adoption, stakeholders warned of a risk that **the compliance burden** on this sector becomes **disproportionate**, while **overall effectiveness remains limited**.

The technological gaps documented in this section are not incidental—they are shaped by the risk environment in which supervisors and obliged entities must operate. Sanctions intensification, instant payments, crypto assets and AI-enabled crime do not merely create new compliance requirements; they set the pace at which technological capability must develop and be sustained. This is what makes the gap consequential: it is not a static deficiency but **one that widens in real time**. Adapting to this fast-moving environment—while simultaneously implementing a major regulatory reform and managing persistent resource constraints—places supervisory systems under **simultaneous and compounding pressure**.

5.3 Challenges in navigating regulatory complexity and change

5.3.1 REGULATORY COMPLEXITY, LEGAL TENSION, AND IMPLEMENTATION PRESSURE

When tackling money laundering, national authorities, FIUs, and private-sector obliged entities operate within a **multi-layered legal environment**, shaped by international standards, EU legislation, and national implementing measures. In practice, risk-mitigation decisions must remain within the boundaries of this wider framework and are not determined by AML/CFT requirements alone.

One of the most operationally significant tensions identified across the Roadshow concerned **the interaction between AML/CFT obligations and data protection requirements**—and it was raised by stakeholders from both the private and public sectors. Financial institutions flagged the friction between AML/CFT monitoring obligations and GDPR constraints around **data sharing and retention** as a **recurring compliance dilemma**: in the view of some stakeholders, complying with one framework may create a risk of breaching the other. FIUs raised a closely related concern in the context of public-private partnerships: the absence of clear guidance on **what data can be shared, with whom, and under which safeguards** is a structural obstacle to implementing information-sharing arrangements consistently and at scale. In both cases, the problem is not a lack of willingness to cooperate, but a need for **greater legal and operational clarity** to ensure **information exchange is lawful, proportionate and auditable**. Clearer guidance on the interaction between AML/CFT obligations and data protection law was one of the most consistent requests directed at AMLA across the Roadshow.

A distinct but related pressure point emphasised during the Roadshow concerned **the ambitious implementation timeline** under the new EU AML/CFT framework. Stakeholders from both the private and the public sector noted that **Level 1 requirements** will become applicable, or will need to be transposed and operationalised, within **a relatively compressed timeframe**, along with a detailed technical framework developed through Regulatory Technical Standards (RTS), Implementing Technical Standards (ITS) and guidelines.

Against this backdrop, obliged entities expressed concern about their ability to **prepare systems, controls and governance arrangements** in a timely and meaningful manner.

5.4 What the challenges reveal

Taken together, the challenges identified across the Roadshow **do not constitute a series of isolated issues**—they form **a coherent and mutually reinforcing picture**. Fragmented starting points mean that a common regulatory framework lands on very uneven institutional landscapes. Resource and capability constraints increase the risk that even well-designed obligations translate into **formal compliance rather than effective risk management**. At the same time, the time pressure creates implementation risks, while the pace of technological change means that implementation challenges continue to evolve as institutions seek to respond.

These conditions also set **clear limits**. Neither the reform of the EU AML/CFT framework nor the establishment of AMLA can, on their own, resolve all identified challenges at once. **AMLA is still in its early years of operation** and will progressively build its capacity over time. Moreover, its actions will be guided by, and constrained within, the mandate and instruments defined by the co-legislators.

Within these parameters, AMLA can nevertheless play a crucial role in **fostering supervisory convergence**, supporting more effective and risk-based supervision, and improving coordination among relevant authorities at EU and national level. At the same time, **national authorities will continue to carry primary responsibility for implementation on the ground**. This is particularly the case in promoting AML/CFT awareness, providing guidance and tools to obliged entities, and investing in supervisory capacity-building in less mature sectors.

Given these circumstances, the question is not whether the challenges can be eliminated in their entirety, but where **targeted action can generate the greatest impact**. The opportunities identified in the next chapter are therefore framed **not as a comprehensive solution**, but as a set of areas in which the new AML/CFT framework can most effectively strengthen the functioning of the AML/CFT system under current constraints.

6 From findings to action: opportunities and AMLA's early response

The risks and challenges described above did not leave Roadshow participants pessimistic. They translated into **clear expectations**. Across supervisors, FIUs, and private-sector stakeholders, there was a broadly shared view that the **2024 reform of the EU's AML/CFT framework**—and AMLA's role within it—represents a **genuine opportunity** to address **structural weaknesses** that have been visible, and largely unresolved, for years, while strengthening the Union's capacity to **protect the integrity of its financial system and internal market**. This chapter examines what that opportunity looks like in practice, drawing on the needs expressed by stakeholders during the Roadshow and on the **foundations that AMLA is already putting in place**.

The opportunities highlighted by the stakeholders mostly targeted **concrete challenges or risks** that they faced. However, broadly speaking, they could be categorised either as opportunities stemming from the **structural change of the EU's AML/CFT system** or as optimism that **new avenues for cooperation, coordination and support** would become possible.

The **Single Rulebook**, **enhanced supervisory convergence**, and **AMLA's coordinating mandate** represent a **structural response to a structural problem**. Fragmentation, uneven starting points, and resource constraints are not incidental features of the current system—they are **products of a model** in which 27 Member States have implemented successive AML directives through 27 national frameworks, with **limited mechanisms for convergence and cooperation**. The potential for establishing **clear guidance** on supervision, FIU cooperation, data sharing, common standards for the use of technology, potential pooling of resources among supervisors and/or FIUs (not only on technology), and **promoting capacity building at national level** for less prepared entities or sectors are all opportunities that stakeholders hope will be met.

6.1 The structural change of the EU's AML system: building a level playing field

The Roadshow did not reveal the fragmentation problem—it confirmed how deeply it is felt. The case for a Single Rulebook has been well documented, and stakeholders did not need to be persuaded of it; they arrived having already lived it. What the Roadshow makes clear is that **the appetite for harmonisation is not passive optimism but an active demand**, rooted in the experience of a directive-based framework whose unevenness—through national transposition, divergent supervisory interpretations and inconsistent enforcement—has had **real operational**

and competitive consequences. A more harmonised rulebook is therefore expected not only to increase legal certainty, but to close the gaps that regulatory arbitrage has exploited. In this context, AMLA has been tasked with developing a **substantial set of Level 2 and Level 3 measures** to complete the Single Rulebook—a substantial regulatory programme that will **define the operational character of the new framework.** Notably, AMLA’s **first draft Regulatory Technical Standards** were transmitted to the European Commission in December 2025 and relate to the **risk assessment methodologies** underpinning (i) the **selection of credit and financial institutions** (or groups) for **AMLA’s direct supervision** and (ii) the assessment and classification of obliged entities’ **inherent and residual ML/TF risk profiles.** This milestone marked an important early step towards **more harmonised, data-driven supervision across the Union.**

AMLA has also indicated that it is prioritising standards that are most relevant to the private sector and frame preventive practices across sectors, including those relating to business relationships and customer due diligence. This sequencing matters: the measures delivered first will **set the tone** for how the Single Rulebook is received by obliged entities and will **shape expectations** for what follows.

Stakeholders were clear, however, that the **opportunity is conditional.** The benefits of the Single Rulebook will depend on how these technical standards are designed and applied in practice. **Proportionality and operational workability** were repeatedly identified as decisive, particularly from smaller firms and for parts of the non-financial sector. A rule set calibrated primarily to large, high-risk financial institutions risks imposing disproportionate burdens on entities with fundamentally different risk profiles, business models and capacities. Getting proportionality right was therefore described not as a secondary consideration, but as **a condition of the reform’s credibility** in the eyes of a significant share of obliged entities.

At the same time, stakeholders’ expectations regarding proportionality were not always aligned with the constraints of **Level 1 legislation.** Certain calls for flexibility or even exemptions from AML/CFT obligations would require changes to primary law and therefore **fall outside the scope** of what can be delivered through technical standards or guidance. Within these boundaries, AMLA will seek to make full use of the instruments available to it to support consistent, **risk-based and workable implementation,** but it cannot deviate from or dilute the requirements set by the co-legislators.

Similarly, a clear and shared articulation of the **risk-based approach** was identified as essential. Without this, divergence may re-emerge through differing supervisory practices even under a more harmonised legal framework.

Alongside the Single Rulebook, **supervisory convergence** emerged across the Roadshow as one of the clearest opportunities provided by the new EU AML/CFT framework. The two are closely related but distinct: harmonised rules set the standard, whereas supervisory convergence is what helps ensure that the standard is **interpreted and applied consistently in practice**. Stakeholders drew a clear line between supervisory divergence and competitive distortion, noting that where supervisory approaches, expectations and intensity vary significantly across Member States, firms may face **uneven compliance burdens**, which can affect the **level playing field** and the smooth functioning of the internal market.

AMLA's **convergence mandate** is now beginning to take concrete shape. In practice, supervisory convergence extends well beyond the existence of common rules. It concerns, among other things, how ML/TF risks are mapped, how individual obliged entities are assessed against those risks, how supervisory priorities are set, how activities are planned and resources allocated, how the intensity of supervisory action is calibrated in light of the risk profile of the entity concerned and the follow-up to such action is defined. The legal framework provides AMLA with a set of tools specifically designed to **drive convergence** across those dimensions, including a harmonised AML/CFT supervisory methodology, a common supervisory manual, **supervisory convergence assessments** and **peer reviews** on the activities of national supervisory authorities respectively in the financial and the non-financial sector, as well as support and facilitation of the work of AML/CFT supervisory colleges.

As mentioned above, a central element of this architecture is the **harmonised risk assessment methodology**. In December 2025, AMLA published draft RTS under Article 40(2) of Directive (EU) 2024/1640 (AMLD) that, for the first time, sets out a common methodology for assessing and classifying the **inherent and residual ML/TF risk profile** of financial-sector obliged entities across the Union. AMLA explained that these instruments are intended to ensure that national supervisors and AMLA, when acting as direct supervisor, assess risk through **the same methodological lens**, thereby supporting a more robust and consistent supervisory framework across the Union. This methodology is designed to inform supervisory prioritisation and to help ensure that supervisory resources are directed where risks are higher. AMLA is also developing, in cooperation with national authorities, a **common supervisory manual**, which should further support consistent supervisory practice. This is genuinely aligned with the messages heard during the Roadshow: many supervisors called not simply for common rules, but a **common supervisory culture**, supported by shared methods and a common understanding of risk.

At the same time, a number of well-resourced supervisory authorities were careful to stress that convergence should mean **raising the floor**, not averaging down standards. AMLA's credibility will therefore depend in part on whether it can demonstrate that the harmonisation lifts weaker

supervisory systems toward stronger ones, rather than producing a **lowest-common-denominator outcome**. In this respect, AMLA's indirect supervision and oversight framework is built around **continuous dialogue and close collaboration** with national competent authorities, while its programme also highlights a common risk assessment methodology and a supervisory handbook, mutual assistance and participation in AML/CFT colleges as core instruments for promoting **consistent and high-quality supervisory approaches** across jurisdictions.

Furthermore, AMLA will perform **supervisory convergence assessments** in the financial sector, with initial targeted assessments planned for 2026, and **peer reviews** in the non-financial sector, with a view to precisely identifying best practices, supporting remedial actions where needed, and fostering a culture of continuous improvement across the Union.

FIUs raised convergence in a related but more operational sense: the need to establish **a stronger and more even baseline of analytical and cooperative capacity** across the EU. **AMLA's Support and Coordination Framework for FIUs**—encompassing joint analyses and peer reviews, alongside the transfer and optimisation of **FIU.net**—was widely seen as an important mechanism to strengthen **FIU cooperation and information exchange** over time and to support a more effective network. In this context, the **first joint analyses** will be an important signal of how AMLA intends to exercise its convening and coordination role across the Union's FIU network in practice.

6.2 New avenues for cooperation, coordination and support

6.2.1 PUBLIC-PRIVATE PARTNERSHIPS AND INFORMATION SHARING

Stakeholders identified **public-private partnerships** and more structured **information-sharing** as one of the most promising avenues for strengthening both prevention and detection of money laundering and terrorist financing. Many emphasised the value of **timely data sharing**, access to shared databases and closer interaction with FIUs, which were regarded as a possible step change in the ability to **detect complex or cross-border patterns** that might otherwise remain undetected. Such arrangements were also considered relevant to **narrowing the gap between fraud prevention and AML/CFT efforts**, and to supporting a more **consistent understanding of emerging typologies and risks** across institutions, sectors and jurisdictions.

At the same time, stakeholders noted that the effectiveness of such partnerships will depend on the **practical operationalisation of the new EU framework**, including an appropriate balance between AML/CFT objectives, data protection requirements and the safeguards applicable to information sharing. While some Member States have already gained experience with domestic public-private partnership models, such arrangements have in practice often been constrained by uncertainty as to the **applicable legal basis**, the interaction with data protection requirements

and the **conditions for lawful information exchange**, particularly where personal or operational data are concerned. This has, in turn, limited their scope in some cases, led to deadlocks in others, and generally made it more difficult to achieve consistency across borders.

The 2024 reform now provides an explicit Union-level basis for such exchanges through **Article 75 of the AML Regulation**, which sets out the conditions under which members of partnerships for information sharing may exchange information for AML/CFT purposes, subject to **strict safeguards**. In this context, AMLA recognises the potential of the Article 75 framework in the fight against money laundering and terrorist financing and is actively engaging with relevant stakeholders to support its effective operationalisation. This includes a dedicated workstream involving dialogue with the **European Data Protection Supervisor (EDPS)** and the **European Data Protection Board (EDPB)**, as well as with both national authorities and the private sector, with a view to paving the way for the effective set-up of partnerships for information sharing—including cross-border ones—from 2027 onwards.

6.2.2 TECHNOLOGY AND SHARED INFRASTRUCTURE

Stakeholders consistently framed **technology** not only as a source of risk and operational challenge, but also as a **collective opportunity** to strengthen AML/CFT effectiveness. AMLA's strategic planning places particular emphasis on building the **foundational data and IT backbone** needed to support both its supervisory and FIU-related pillars. This includes the establishment of the **central AML/CFT database** and the progressive transfer and optimisation of **FIU.net**, aimed at enabling a more structured, secure and analytically useful information exchange across the Union. AMLA's programme particularly presents the central AML/CFT database as a **key enabler of supervisory convergence**, by improving risk identification, monitoring and cross-border visibility across national authorities.

Looking ahead, AMLA has also set out a broader **digital roadmap** focused on building and modernising mission-critical systems, strengthening **data analytics capability** and, where appropriate, integrating **AI-enabled solutions** under robust governance arrangements and safeguards. Stakeholders saw this direction as especially relevant for promoting more scalable supervision and effective FIU cooperation, including through shared approaches and improved interoperability.

At the same time, AMLA's immediate focus is not on providing a broad suite of operational tools. Rather, its near-term priority is to establish the **core infrastructure, data capabilities and coordination mechanisms** on which a more technology-enabled EU AML/CFT system can progressively be built. Over time, this may create scope for a wider ecosystem of **shared solutions**

and practical tools, but in the short term the emphasis remains on **foundational systems** and on supporting national authorities.

In this respect, the development of **common data and tools for national authorities** may itself become a powerful **driver of convergence** in the future. By equipping supervisors with more consistent sources of information, shared risk indicators and increasingly comparable technological capabilities, AMLA's digital work may help reduce fragmentation in supervisory practices and support a more coherent Union-wide approach. In the near term, AMLA's planned focus on **higher-risk and cross-border areas**, including the crypto-asset market, may provide an early test of how EU-level technology-enabled data and coordination can strengthen the collective capacity of national supervisors and FIUs to **detect cross-border patterns** and respond more consistently to fast-evolving risks.

6.2.3 CAPACITY BUILDING

Particularly in the non-financial sector, AMLA was identified as a **long-term enabler of capability** rather than merely a rule-setter. National supervisors pointed to the value of **AMLA-led guidance**, common supervisory approaches, and **training frameworks** in sectors where the **gap between regulatory expectation and operational reality** remains most pronounced. Private-sector stakeholders similarly emphasised that **practically oriented guidance** can be an important lever for raising awareness and effectiveness in a part of the obliged-entity population that has historically received less tailored support than the financial sector.

At the same time, **capacity-building for obliged entities themselves would remain primarily a matter for national authorities**. AMLA's role is better understood as **supporting that effort indirectly**, by fostering supervisory convergence and strengthening the capabilities of national competent authorities. In its 2026–2028 programme, AMLA presents capacity-building as part of its longer-term effort to enhance the overall effectiveness of the EU AML/CFT system, including through sectoral and cross-sectoral training, supervisory guidance and support for the exchange of best practices. In particular, AMLA foresees **targeted training activities already in 2026** and, in the non-financial sector, the development of a roadmap for training programmes and the delivery of **first training sessions for supervisory authorities**. This suggests that AMLA's most immediate contribution will be to **equip national supervisors more effectively**, while any wider awareness-raising and operational support for obliged entities will continue to be channelled primarily through national supervisory frameworks.

6.3 The work ahead

Throughout 2025, AMLA has described itself, accurately, as a **start-up**—an institution with a clear vision and a detailed plan, but at the beginning of a long journey. The Roadshow confirmed both the scale of what needs to be built and the fact that building it is a **shared endeavour**. The opportunities identified by stakeholders across 27 Member States are **not guaranteed to materialise**—they are conditional on AMLA’s choices about **proportionality in the Single Rulebook, ambition in supervisory convergence, clarity on data sharing, and investment in shared infrastructure and capacity building**.

What the Roadshow demonstrated above all is that the **conditions for a genuinely effective EU-wide AML/CFT system** exist for the first time—in the **legal architecture of the AML package**, in the **institutional mandate of AMLA**, and in the broadly shared willingness of supervisors, FIUs, and private-sector actors to engage as partners in making it work. The five themes that run through this report converge at this point: the changing risk landscape makes the case for why **the reform was necessary**; the different starting points define the scale of the convergence challenge; technology shapes both the threats and the tools available to address them; the structural reform provides the framework; and the expectations towards AMLA define the role it is being asked to play. How well that role is fulfilled will determine whether the opportunity the reform represents is realised.

Contact information



**AUTHORITY FOR ANTI-MONEY LAUNDERING AND
COUNTERING THE FINANCING OF TERRORISM**

MesseTurm, Friedrich-Ebert-Anlage 49
60308 Frankfurt am Main, GERMANY

<https://www.aml.eu/>