Regulation

MiCA - Key Tasks and Deadlines

The depth and scale of MiCA are daunting for many crypto businesses. Compliance will require investment in time and resources, as deadlines vary between European jurisdictions, and there is a whole new vocabulary to learn.

BCB's compliance and legal team have recently completed our own MiCA application and continue to hold regular discussions with clients about what MICA will mean for them. While the new regulatory regime cannot be captured in a single page, there are six key steps that firms will need to address to meet the challenges and opportunities that MiCA presents.

Stablecoins

Some stablecoins will not meet the requirements of MiCA

And firms offering services in these coins will need to delist them. Tether's USDT is the best-known example, but the effective ban will apply to other stablecoins. Firms will need to check and delist all non-MiCA compliance stablecoins.

Strengthen IT Security & Operational Resilience

This includes all RegTech, trading solutions and a monitoring framework.

Monitoring is particularly important for trading teams, which will not be used to having such a framework. Requirements vary, but price monitoring is a key requirement to ensure investor protection, which is the top priority for regulators.

- Develop a cybersecurity framework to protect customer assets and private keys.
- Implement incident reporting mechanisms to regulators for security breaches.
- Establish business continuity and disaster recovery plans to prevent service disruptions.
- Ensure compliance with DORA (Digital Operational Resilience Act), which applies to financial entities in the EU.

Cybersecurity Audit

Firms will need a lot more certification and, specifically, an audit by an approved third-party provider.

In France, for example, these must be carried out by a provider that is registered as a Prestataires d'audit de la sécurité des systèmes d'information (PASSI). Standards are based on the Digital Operational Resilience Act (DORA), which came into effect this year and set standards of digital systems and security for all financial institutions

Anti-money Laundering

Essential AML standards do not change.

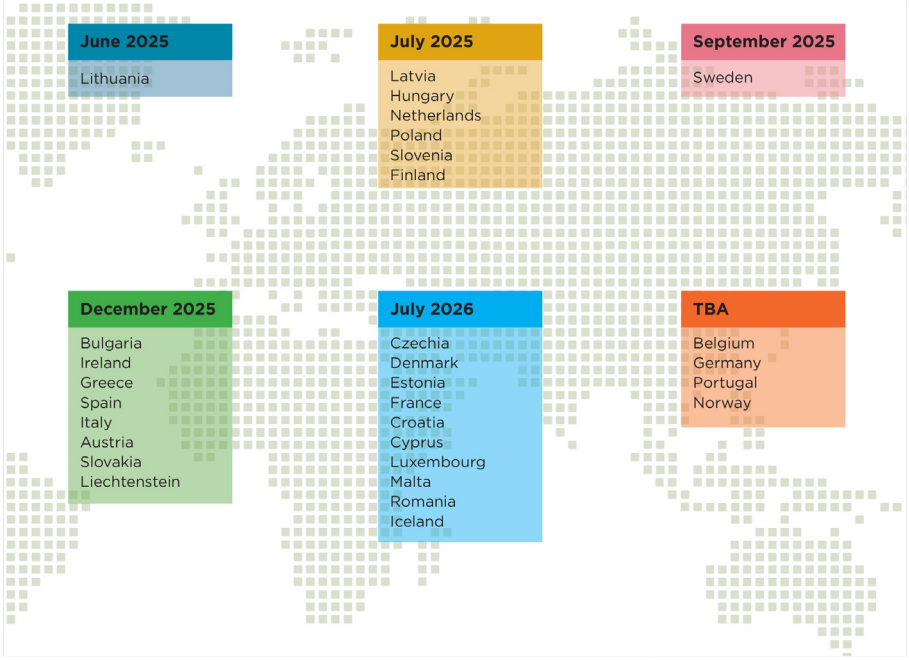
The key difference is the Travel Rule which requires the sharing of client information for transactions over a certain level. Every originator and beneficiary for every transaction have to be identified each time, through a secure system that harmonises the information. Clients in such transactions will be required to provide ID including pictures or video.

- Implement a robust AML/CFT policy that meets AMLD6 and FATF requirements.
- Deploy a risk-based approach (RBA) for client onboarding and ongoing transaction monitoring.
- Integrate Travel Rule compliance into transaction processing (mandatory for all CASPs).
- Appoint a Money Laundering Reporting Officer (MLRO) and ensure they have relevant experience.

BCB GROUP

Secure Your Governance, Internal Controls & Capital Requirements

Named individuals must be assigned certain roles and responsibilities at any offer or firm, covering a range of key responsibilities including IT, communications security and cryptographic keys. These roles and responsibilities must be identified in every EU and European Economic Area (EEA) jurisdiction where the firm has an entity. Group-wide governance will not be sufficient to meet these requirements.



Capital Reserves for Issuers

Reserve assets must be kept separate from the issuer's other funds. The state of these reserves must be reported regularly to relevant authorities.

CASPs that do not issue ARTs are also subject to capital adequacy requirements. These requirements will vary based on the specific services offered and the risk profile of the CASP. The competent authorities in each EU member state will determine the appropriate level of capital required, ensuring it is adequate to cover potential operational and financial risks.

This may include requirements for initial capital, ongoing capital maintenance, and liquidity buffers." specific capital adequacy requirements applicable in each jurisdiction where the CASP operates. The exact capital requirements for non-issuing CASPs are not a fixed number but rather a variable amount decided by local regulators, taking into account the individual CASP's activities and the associated risks.

A base capital requirement of €350,000 applies to all issuers of Asset Referenced Tokens (ART). Issuers must also hold capital equivalent to 2% of the average value of their reserve assets.

Deadlines

MiCA came into force in December 2024, but firms already operating under existing laws will be able to continue their activities until they become MiCA-compliant.

Called the "grand fathering" period, EU member states have put in place different deadlines varying from 5 months to 18 months from the entry in force of MiCA on December 30th 2024, so the exact date you need to be MiCA compliant depends on your jurisdiction.

Final thought: Be Proactive, Not Reactive

Navigating the MiCA licensing process requires careful planning and execution By focusing on these five key areas – technical infrastructure, AML compliance, cybersecurity, capital reserves, and governance – CASPs can significantly enhance their chances of a successful application. The investment in time and resources is substantial, but it is essential for operating within the new regulatory framework and building trust with clients.

BCB GROUP