European Crypto Initiative

MiCA Booklet

Read MiCA with EUCI

Table of Contents

Table of Contents

Table of Contents

I. Introduction

As part of our "Read MiCA with EUCI" project, we have created a more readable and user-friendly overview of the MiCA regulation. The aim of this document is to make the first regulation on crypto-assets accessible to all users and help in understanding the regulation itself. The document is divided into several chapters, following the structure of the MiCA regulation, providing a comprehensive and clearer treatment of all the key topics covered by the regulation.

II. Overview of MiCA's objectives and significance

The Markets in Crypto-assets (MiCA) Regulation was proposed by the European Commission on 24 September 2020. This proposal was part of the broader Digital Finance Package, which aimed to create a comprehensive regulatory framework for digital finance within the European Union.

The final version of MiCA was published in the Official Journal of the European Union on 9 June 2023, marking its official finalisation. MiCA officially came into force in June 2023, with its provisions set to become fully applicable in 2024. The regulation first applied to stablecoins on 30 June 2024, followed by its complete implementation across all areas on 30 December 2024. MiCA is designed to enhance market integrity and financial stability by establishing comprehensive regulations for issuers and service providers operating within the crypto-asset space.

MiCA addresses several critical areas to achieve its objectives. It mandates strict transparency and disclosure requirements for the issuance, public offering, and admission of crypto-assets to trading platforms (as outlined in MiCA Title II). The regulation also sets forth robust standards for the authorisation and supervision of crypto-asset service providers (CASPs) under MiCA Title V, as well as for issuers of stablecoins—referred to as "asset-referenced tokens" (ARTs) and "e-money tokens" (EMTs)—detailing their operational, organisational, and governance structures (MiCA Titles III and IV). Additionally, MiCA introduces essential measures to prevent insider trading, unlawful disclosure of inside information, and market manipulation, ensuring the integrity of crypto-asset markets (MiCA Title VI).

The MiCA Regulation proposed by the European Commission represents a critical legislative initiative to regulate the rapidly evolving crypto-asset market within the European Union (EU). As part of the broader Digital Finance Package, MiCA's primary objective is to create a comprehensive and harmonised regulatory framework that fosters innovation, ensures legal certainty, and addresses the risks associated with crypto assets.

This initiative aligns with the EU's broader goals of embracing digital transformation and building a resilient, future-ready economy that works for all citizens and businesses across its member states.

Objectives of MiCA

1. Legal Certainty and Harmonization: The foremost objective of MiCA is to establish legal clarity in the treatment of crypto-assets. As the crypto-asset market has expanded, the fragmentation of regulations across different EU member states has created significant legal uncertainty, hampering the ability of businesses and investors to engage confidently in the market. MiCA addresses this challenge by providing a clear and consistent legal framework applicable across the EU, ensuring that all crypto assets not covered by existing financial services legislation are appropriately regulated (for example, all crypto assets that fall under the financial instruments framework are outside MiCA's scope). This harmonisation of rules is critical for enabling cross-border activities, reducing legal and regulatory complexity, and lowering costs for market participants, thereby facilitating the development and expansion of crypto-asset activities throughout the Union.

2. Supporting Innovation and Competitiveness: MiCA is designed to strike a balance between regulation and innovation, supporting the development and adoption of Distributed Ledger Technology (DLT) and crypto-assets within a safe and proportionate regulatory environment. By fostering a competitive market, MiCA aims to position the EU as a global leader in the emerging crypto-asset industry. The regulation encourages innovation by creating a flexible framework that accommodates future technological advancements and the growth of the market, ensuring that European firms can lead in the digital finance space without being stifled by overly restrictive regulations. This approach is aligned with the EU's broader goal of digital sovereignty, which seeks to maintain Europe's competitiveness in the global digital economy.

3. Consumer and Investor Protection: Another key objective of MiCA is to enhance consumer and investor protection. While crypto-assets offer significant opportunities, they also pose some risks that are similar to traditional financial instruments, including market volatility, fraud, and the potential for substantial financial losses. MiCA addresses these concerns by establishing clear rules for transparency, disclosure, and accountability, which aim to protect consumers and investors from these risks. The regulation introduces transparency and disclosure requirements for the issuance, public offering, and trading of crypto-assets, ensuring that market participants have access to critical information.

This protection is particularly important in a market where traditional safeguards may not apply, leaving participants vulnerable to new and emerging threats.

4. Financial Stability and Market Integrity: MiCA also focuses on maintaining financial stability within the EU and ensuring the integrity of crypto-asset markets. The regulation acknowledges the potential systemic risks posed by certain crypto-assets, particularly stablecoins, which could become widely adopted and impact the broader financial system. To mitigate these risks, MiCA introduces specific provisions for the authorisation, supervision, and governance of stablecoin issuers, known according to MiCA as issuers of asset-referenced tokens (ARTs) and e-money tokens (EMTs). These provisions are designed to prevent any potential disruptions to financial stability or the effectiveness of monetary policy that could arise from the rapid growth of stablecoins. Additionally, MiCA establishes measures to prevent insider dealing, unlawful disclosure of inside information, and market manipulation, thereby ensuring that the crypto-asset markets operate fairly and transparently.

Significance of MiCA

The significance of MiCA extends beyond its immediate regulatory impact. By creating a unified regulatory framework, MiCA addresses the fragmentation and inconsistencies that have historically plagued the crypto-asset market in the EU. This harmonisation is crucial for enabling cross-border activities, reducing legal and regulatory complexity, and lowering costs for market participants. Moreover, by providing a clear legal foundation, MiCA facilitates greater access to capital and financial services for businesses operating in the crypto-asset space, which has traditionally been a challenge due to regulatory uncertainties.

MiCA is also significant in promoting the EU's strategic objectives in digital finance and blockchain technology. By supporting the adoption of these technologies, MiCA contributes to the EU's broader goal of digital sovereignty, ensuring that Europe remains at the forefront of global digital innovation. The regulation also complements other EU initiatives aimed at building a robust digital economy, including the Capital Markets Union (CMU) and the European Blockchain Strategy.

Furthermore, MiCA's approach to consumer and investor protection sets a high standard for the global crypto-asset market. By prioritising transparency, fairness, and accountability, MiCA serves as a model for other jurisdictions seeking to regulate crypto assets in a way that balances innovation with risk management. The regulation's focus on financial stability also reflects the EU's commitment to safeguarding its financial system against potential disruptions from new and emerging financial technologies.

MiCA also introduces important rules regarding reverse solicitation and cross-border market access by third-country firms. The regulation restricts third-country firms from soliciting clients in the EU without complying with the authorisation requirements, effectively setting a marketing ban. However, exceptions exist under the principle of reverse solicitation, where the client initiates the contact, allowing third-country providers to offer specific services based on the client's initiative. This aspect of MiCA reflects the regulation's attention to ensuring that EU markets are protected from unregulated external influences while allowing flexibility in cross-border financial services.

In conclusion, MiCA is a landmark regulation that not only addresses the immediate challenges of regulating the crypto-asset market but also lays the foundation for the future of digital finance in the EU. By providing legal certainty, supporting innovation, protecting consumers and investors, and ensuring financial stability, MiCA is poised to play a pivotal role in shaping the development of the crypto-asset industry within the EU and beyond. The regulation's comprehensive approach reflects the EU's ambition to lead in the global digital economy while safeguarding the interests of its citizens and businesses.

III. Overview of Asset-referenced tokens [1]

1. Authorisation

Asset-referenced tokens can be offered to the public or traded within the Union if the issuer of the token is:
(a) **a legal entity or equivalent undertaking established in the Union and authorised by the home Member State's competent authority.** Other undertakings may issue such tokens only if their legal form provides protection for third parties equivalent to that of legal persons and if they are subject to equivalent prudential supervision appropriate to their legal form;
(b) **a credit institution**;
(c) **other individuals if they comply with:**

- Obligation to act honestly, fairly, and professionally in the best interest of the holders of asset-referenced tokens,
- Marketing communications,
- Prohibition of granting interest.

Issuing is only permitted for entities that are not formed as legal persons if their legal structure provides third-party interest protection equivalent to that of legal entities and they are under appropriate prudential supervision.

Authorisation granted under point (a) is valid throughout the Union, allowing the issuer to offer the authorised asset-referenced token to the public or seek its trading admission Union-wide.

Exceptions from Requirements

The above requirements do not apply if:

(a) The average outstanding value of the asset-referenced tokens issued does not exceed 5 million EUR (or its equivalent in another currency) over any 12-month period ending daily, and the issuer is not part of a network of exempt issuers; or
(b) The tokens are exclusively offered to and held by qualified investors.

The exempt crypto-asset issuers from point (a) and point (b) must prepare a

---

1 The provisions on Asset-referenced tokens in the Markets in Crypto-assets (MiCA) Regulation are contained in Title III, Articles 16 to 47, Annex II Annex V.

white paper (as outlined in chapter 2 below), and submit it, along with any related marketing materials, to the competent authority of their home Member State. The competent authority's approval of a crypto-asset issuer's white paper is also valid throughout the Union.

1.2. Application for Authorisation

Legal entities or other organisations planning to offer asset-referenced tokens to the public or seek their trading admission must submit their authorisation application to the competent authority in their home Member State.

Upon receiving an application as described below, the competent authority must formally acknowledge its receipt in writing to the applicant issuer within two working days.

The application must include the following comprehensive information:

(a) the issuer's address;
(b) the legal entity identifier of the issuer;
(c) the issuer's articles of association, if applicable;
(d) a business model outline detailing the operational plans the issuer intends to pursue;
(e) a legal opinion confirming the asset-referenced token does not fall under the excluded categories (such as financial instruments, deposits, funds, securitisation positions, non-life or life insurance products, pension products, officially recognised occupational pension schemes, individual pension products, a pan-European Personal Pension Product, or social security schemes) or qualify as an e-money token;
(f) an in-depth description of the governance structures. Issuers of asset-referenced tokens shall have robust governance arrangements, including a clear organisational structure with well-defined, transparent, and consistent lines of responsibility; effective processes for identifying, managing, monitoring, and reporting the risks to which they are or may be exposed; and adequate internal control mechanisms, including sound administrative and accounting procedures;
(g) if applicable, descriptions of cooperation with specific crypto-asset service providers, including their internal controls and procedures for adhering to anti-money laundering and counter-terrorism financing obligations under Directive (EU) 2015/849[2];

2 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

(h) identities of the management team members;
(i) evidence verifying the good reputation and relevant knowledge, skills, and experience of the management team;
(j) verification of the good reputation of any direct or indirect shareholder or member with a significant stake in the issuer;
(k) a crypto-asset white paper;
(l) documentation of policies and procedures;
(m) descriptions of contractual engagements with third-party entities. Where issuers of asset-referenced tokens enter into arrangements as referred to in point (l) above, those arrangements shall be set out in a contract with the third-party entities. Those contractual arrangements shall specify the roles, responsibilities, rights, and obligations of both the issuers of asset-referenced tokens and the third-party entities. Any contractual arrangement with cross-jurisdictional implications shall provide for an unambiguous choice of applicable law;
(n) an outline of the issuer's business continuity policy. Issuers of asset-referenced tokens shall establish a business continuity policy and plans to ensure, in the event of an interruption of their ICT systems and procedures, the preservation of essential data and functions and the maintenance of their activities or, where this is not possible, the timely recovery of such data and functions and the timely resumption of their activities;
(o) details of internal control mechanisms and risk management procedures. Issuers of asset-referenced tokens shall have in place internal control mechanisms and effective risk management procedures, including effective control and security arrangements for the management of ICT systems as required by Regulation (EU) 2022/2554[3] of the European Parliament and of the Council. These procedures shall include a comprehensive assessment of the reliance on third parties for the operation of the reserve, the investment of the reserve, the custody of the reserve and, where applicable, the distribution of the asset-referenced tokens to the public. Issuers of asset-referenced tokens shall regularly monitor and evaluate the adequacy and effectiveness of the internal control mechanisms and risk assessment procedures and take appropriate measures to address any deficiencies in this respect;
(p) descriptions of systems and processes designed to ensure the data's availability, authenticity, integrity, and confidentiality. Issuers of asset-referenced tokens shall have in place systems and procedures adequate to ensure the availability, authenticity, integrity, and confidentiality of data as required by Regulation (EU) 2022/2554. These systems shall record and safeguard relevant data and information collected and generated in the

3 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

course of the issuers' activities;
(q) a description of the issuer's procedures for handling complaints;
(r) where relevant, a list of host Member States where the issuer plans to offer the asset-referenced token to the public or seek its trading admission.

Governance Arrangements

A) Documentation of Policies and Procedures

1. **Reserve of Assets:** Policies concerning the reserve of assets.
2. **Custody of Reserve Assets:** Procedures for the custody and segregation of reserve assets.
3. **Rights of Token Holders:** Documentation on the rights granted to holders of asset-referenced tokens.
4. **Issuance and Redemption Mechanisms:** Details on the processes for issuing and redeeming tokens.
5. **Transaction Validation Protocols:** Protocols for validating transactions involving asset-referenced tokens.
6. **Distributed Ledger Technology:** Functionality and operations of the issuer's proprietary distributed ledger technology or similar technology, whether managed by the issuer or a third party.
7. **Liquidity Mechanisms:** Mechanisms ensuring the liquidity of asset-referenced tokens, including the liquidity management policies and procedures, especially for issuers of significant tokens.
8. **Third-Party Arrangements:** Arrangements with third-party entities regarding the operation, investment, and custody of the reserve assets and, where applicable, the distribution of the tokens to the public.
9. **Consent for Trading Admission:** Written consent from the issuer for others to offer or seek the admission of asset-referenced tokens to trading.
10. **Complaints-Handling:** Procedures for handling complaints.
11. **Conflicts of Interest:** Policies to manage conflicts of interest.

Governance Arrangements for Issuers of Asset-Referenced Tokens

Issuers of asset-referenced tokens are required to maintain robust governance structures, including clear organisational lines of responsibility, effective risk management, and solid internal controls.

Management Body Responsibilities:

Assessment and Review: The management body must regularly assess and review the effectiveness of policies, procedures, and arrangements to ensure compliance with Chapters 2, 3, 5, and 6 of this Title of MiCA.

Any deficiencies identified must be addressed promptly.

- **Reputation and Expertise:** Members of the management body must be of good repute and possess the necessary knowledge, skills, and experience to perform their roles. They must not have any convictions related to money laundering, terrorist financing, or other offences that could impair their reputation. Additionally, they must demonstrate a commitment to dedicating sufficient time to fulfil their responsibilities effectively.

Shareholder and Member Requirements:

- **Reputation:** Shareholders or members holding qualifying stakes in the issuer must also be of good repute and free from convictions related to money laundering or terrorist financing offences.

(B) Proving Good Reputation, Relevant Knowledge, and Experience

Issuers of asset-referenced tokens must provide evidence verifying the good reputation, knowledge, skills, and experience of their management team, as well as the good reputation of any significant shareholders or members.

Re-submission of Information:

- Issuers already authorised for one asset-referenced token do not need to resubmit identical information for another token's authorisation. However, they must affirm that all previously submitted information remains current and accurate.

Requirements for the Applicant Issuer:

- **Criminal Record Check:** Each member of the management body must have no criminal record related to commercial, insolvency, or financial services laws, nor offences involving anti-money laundering, counter-terrorist financing, fraud, or professional liability.
- **Collective Competence:** The management body must collectively possess the necessary knowledge, skills, and experience to manage the issuer effectively. They are required to dedicate adequate time to fulfil their responsibilities.
- **Shareholder and Member Checks:** All shareholders and members with significant holdings, whether direct or indirect, must have no criminal record related to the aforementioned areas.

(C) Complaints-Handling Procedures

Issuers of asset-referenced tokens must establish fair and consistent procedures for handling complaints from token holders and other interested parties. These procedures must be published and made accessible to the public.

Third-Party Involvement:

- If third parties are involved in managing the reserve of assets or distributing the tokens, issuers must have specific procedures to handle complaints between holders and these third parties.

Filing and Handling Complaints:

- **Complaint Submission:** Token holders can file complaints directly with the issuer or the relevant third party.
- **Template Availability:** Issuers must provide a template for filing complaints and maintain a record of all complaints and actions taken in response.
- **Investigation and Response:** Issuers are required to investigate and respond to complaints fairly and promptly.

EBA and ESMA's Regulatory Technical Standards

- The European Banking Authority (EBA) submitted its regulatory technical standards. These standards specify the requirements, templates, and procedures for handling complaints under the Markets in Crypto-assets Regulation (EU) 2023/1114.
- The European Securities and Markets Authority (ESMA) draft regulatory technical standards explaining how complaints should be handled. The Commission may adopt additional standards based on these drafts in accordance with Regulation (EU) No 1093/2010[4].

(D) Reserve of Assets

Reserve Requirements for Issuers

Issuers of asset-referenced tokens must maintain a reserve of assets managed to:

- Cover risks associated with the assets referenced by the tokens.
- Address liquidity risks related to the permanent redemption rights of token holders.

Segregation of Assets

The reserve must be kept separate from the issuer's assets and other tokens to protect token holders, particularly in cases of bankruptcy.

---

4 Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC.

Issuers offering multiple asset-referenced tokens must manage separate pools of assets for each token. However, if different issuers offer the same token, only one pool of assets is required.

Effective Management

Managers must ensure that the reserve of assets is managed carefully, with issuance and redemption of tokens always corresponding to changes in the reserve. The reserve's value must be determined using market prices and must at least equal the value of claims from token holders.

Stabilisation Policy

Issuers must have a stabilisation policy for their tokens, detailing:

- The composition and list of assets.
- Description of assets in the reserve.
- Risk assessment of the reserve.
- Issuance and redemption processes and their impact on the reserve.
- Investment of any part of the reserve, including the investment policy and its effect on reserve value.
- Procedures for purchasing and redeeming tokens.

Auditing

Regular Audits
Issuers must undergo regular audits by independent auditors every six months. These audits assess compliance with reserve management rules. Results must be reported to the management body and the competent authority and published within two weeks unless delayed by the authority for specific reasons, such as protecting the financial system or token holders.

Valuation

Market Valuation
The reserve of assets must be valued at market prices using a mark-to-market approach, favouring the cautious side of the bid and offer. This valuation should consider:

- The number and quality of counterparties.
- Market volume and turnover.
- The size of the reserve.

If market data is insufficient, a mark-to-model approach is used to estimate

intrinsic value, considering market volume, turnover, and risks associated with the reserve asset. The amortised cost method is not permitted under this approach.

EBA and ESMA's Regulatory Technical Standards

Development of Standards
The European Banking Authority (EBA) draft regulatory technical standards on liquidity requirements for the reserve of assets, including:

- Percentage of asset reserves based on maturity.
- Minimum deposits in official currencies.
- Other liquidity management techniques.

(E) Conflicts of Interest

Identification

Issuers of asset-referenced tokens must implement and maintain effective policies and procedures to identify, prevent, manage, and disclose conflicts of interest between themselves and:

- Their shareholders or members.
- Any direct or indirect shareholder or member with a qualifying holding in the issuer.
- Members of their management body.
- Their employees.
- Holders of asset-referenced tokens.
- Any third party involved in the operation, investment, custody, or distribution of the reserve assets.

Prevention

Issuers must take appropriate steps to:

- Identify, prevent, manage, and disclose conflicts of interest, particularly those related to the management and investment of the reserve of assets.
- Clearly disclose the general nature and sources of conflicts of interest and the steps taken to mitigate them on their website, allowing potential buyers to make informed decisions.

EBA's Regulatory Technical Standards
The European Banking Authority (EBA) drafted technical standards to:

- Specify the requirements for the policies and procedures related to conflicts of interest.
- Detail the content and methodology for the required disclosures.

See also ESMA's draft regulatory technical standards to explain how to handle conflicts of interests.

(F) Mechanisms to Ensure the Liquidity of Asset-Referenced Tokens

Risk Management Policy for Significant Tokens

Issuers of significant asset-referenced tokens must implement a risk management policy that ensures these tokens can be held by various crypto-asset service providers on a fair, reasonable, and non-discriminatory basis.

Liquidity Management and Stress Testing Requirements

Issuers must:

- Assess and monitor liquidity to meet redemption requests.
- Establish and implement a liquidity management policy that ensures the reserve assets have a resilient liquidity profile, enabling normal operations even under stress.
- Conduct regular liquidity stress tests. Based on these tests, the EBA may require increased liquidity.

These requirements apply to each issuer offering significant asset-referenced tokens or multiple tokens within the Union.

Development of Regulatory Standards and Guidelines

The EBA and ESMA are developing standards covering:

1. Bank regulation.
2. Governance arrangements for remuneration policy.
3. Liquidity management policy and procedures, including currency restrictions.
4. Adjustment procedures for the own funds of significant asset-referenced token issuers.

The EBA, in collaboration with ESMA and the ECB, will issue guidelines for stress test scenarios, which will be updated periodically.

(G) Rights Granted to the Holders of Asset-Referenced Tokens

Redemption Rights

Holders of asset-referenced tokens have the right to request repayment at any time if the issuer fails to meet its obligations. Issuers must have a clear policy detailing this redemption process. If a holder requests redemption, the issuer must either:

- Pay the market value of the assets.
- Deliver the assets directly.

Issuers must outline their policy regarding the permanent right of redemption, including:

- Conditions for exercising the right.
- Mechanisms and procedures for redemption, especially during stressed market conditions, including recovery and redemption plans.
- Valuation of tokens and reserve assets using mark-to-market methodology.
- How redemption is settled.
- How the reserve of assets is managed to prevent market disruption.

Issuers must offer redemption in the same currency as the initial payment and cannot charge redemption fees.

(H) Custody of the Reserve Assets, Including the Segregation of Assets

Custodial Requirements

Issuers of asset-referenced tokens must establish policies, procedures, and contracts to ensure:

- Reserve assets are not pledged as collateral.
- Reserve assets are securely held in custody.
- Issuers can access reserve assets quickly for redemption requests.
- Custodians and reserve assets are not concentrated in one place or entity.

Each pool of reserve assets must have its own custody policy, and different issuers must maintain a single custody policy.

Asset Management

Reserve assets must be held in custody within five working days of issuing the tokens.

Custody can be managed by:

- Crypto-asset service providers for crypto-assets.
- Credit institutions for all types of reserve assets.
- Investment firms for financial instruments.

Issuers must select, appoint, and regularly review these custodians to ensure they have the necessary expertise and reputation. Contracts must protect reserve assets from custodians' creditors and detail how custodians are chosen and reviewed.

Custodians must ensure reserve assets are kept safe by:

- Holding funds in segregated accounts.
- Registering financial instruments in segregated accounts.
- Keeping a register of crypto-asset positions.
- Verifying the ownership of reserve assets.

Contractual Obligations
Contracts between issuers and custodians must outline the roles, responsibilities, rights, and obligations of both parties. These contracts must also address cross-jurisdictional issues and ensure that custodians act honestly, fairly, professionally, and in the interest of token issuers and holders, avoiding conflicts of interest.

Liability
If a financial instrument or crypto-asset is lost, the custodian must replace it with an identical or corresponding asset. Custodians are not liable if the loss was caused by an external event beyond their control.

1.3. Application Assessment

- **Initial Review:** Authorities have 25 working days to verify if the authorisation application is complete. If any information is missing, they will promptly notify the applicant issuer.

- **Incomplete Applications:** The authorities will set a deadline for the applicant to provide the missing information. The application, including the crypto-asset white paper, must be complete for the assessment to proceed.

Authorisation Process

- **Assessment Timeline:** The authorities have 60 days to decide on the authorization after receiving a complete application. They may request additional information during this period.
- **Suspension of Assessment:** The 60-day assessment period is paused for 20 working days when authorities request missing information. This suspension does not extend if further information is requested.
- **Draft Decision:** After 60 days, the authorities must send their draft decision and the application to the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), and the European Central Bank (ECB). If the applicant ssuer is based in a non-euro country or the euro is referenced in the token, the draft decision and application must also be sent to the relevant central bank.

Issuer Evaluation and Risk Assessment

- **EBA and ESMA:** These authorities must provide their opinions within 20 working days upon request. They will assess if the asset-referenced token falls under excluded categories or is an e-money token and share their opinions with the competent authority.
- **ECB or Central Bank:** They must give their opinion within 20 working days, focusing on the potential risks to financial stability and payment systems. Their opinion is also shared with the competent authority.
- **Non-Binding Opinions:** While EBA, ESMA, and ECB opinions are not binding, they must be considered by the competent authority during their decision-making process.

1.4. Grant or Refusal of Authorization

- **Authority Decision:** Competent authorities must decide on the authorisation within 25 days of receiving opinions from EBA, ESMA, and the ECB or relevant central bank. They must inform the applicant issuer within five days of their decision.
- **Approval:** If authorisation is granted, the applicant issuer's white paper is approved.

Competent authorities must refuse authorisation if there is clear evidence of:

(a) **Management Risks:** The management body might threaten effective management, business continuity, client interests, or market integrity.
(b) **Criteria Non-Compliance:** Management body members do not meet the required criteria outlined in Chapter 1.2.

(c) **Shareholder Criteria:** Shareholders or members with qualifying holdings do not meet the criteria from Chapter 1.2.
(d) **Regulatory Requirements:** The applicant issuer fails to meet the necessary requirements.
(e) **Business Model Risks:** The business model poses serious risks to market integrity, financial stability, and payment system operation or is prone to money laundering and terrorist financing.

Guidelines and Opinions

- **Guidelines Issuance:** EBA and ESMA jointly issued guidelines on assessing the suitability of management body members and shareholders with qualifying holdings in issuers of asset-referenced tokens.
- **ECB/Central Bank Opinion:** Authorization may be refused if the ECB or relevant central bank provides a negative opinion due to risks to payment systems, monetary policy, or monetary sovereignty.

Post-Authorization Steps

- **Communication:** Competent authorities must notify the single point of contact in the host Member States, ESMA, EBA, the ECB, and, where applicable, the central bank within two working days of granting authorisation.
- **Public Register:** ESMA must update the public register with this information by the start date of the public offer or trading admission.

1.5. Withdrawal of Authorization

Competent authorities must withdraw the authorisation of an issuer of an asset-referenced token under the following conditions:

a. Operational Cessation: The issuer has ceased operations for six consecutive months or has not used its authorisation for 12 consecutive months.
b. Irregular Means: The authorisation was obtained through irregular means, such as false statements in the application or white paper.
c. Non-Compliance: The issuer no longer meets the conditions for which the authorisation was granted.
d. Serious Infractions: The issuer has seriously breached relevant provisions.
e. Redemption Plan: The issuer has been subjected to a redemption plan.
f. Voluntary Renunciation: The issuer has explicitly renounced its authorisation or decided to cease operations.
g.Threats to Stability: The issuer's activities pose a serious threat to market

integrity, financial stability, and payment systems or involve serious risks of money laundering and terrorist financing.

Notification Requirements

- The issuer must notify competent authorities if it is subject to a redemption plan or voluntarily ceases operations.
- Competent authorities must also withdraw authorisation if the ECB or relevant central bank determines that the token threatens payment systems, monetary policy, or monetary sovereignty.

Regulatory Actions

- **Limits on Issuance:** If the ECB or central bank identifies threats, competent authorities may impose limits on the amount or minimum denomination of the token.
- **Third-Party Notifications:** Competent authorities must notify if a third party associated with the issuer loses its relevant authorisation or if management body members or shareholders violate national laws transposing Directive (EU) 2015/849 [5].
- **Reputational and Governance Issues:** Authorization may be withdrawn if there are concerns about the reputation of the issuer's management body or shareholders or if there are governance failures.

Post-Withdrawal Procedures

- **Notification to ESMA:** Competent authorities must notify ESMA of the authorisation withdrawal within two working days. ESMA will update the register without delay.

1.6. Specific Requirements for Credit Institutions

Authorisation and Compliance

- **Existing Authorization: Credit institutions authorised** under Directive 2013/36/EU [6] do not need additional authorisation under the MiCA Regulation to offer or seek admission for asset-referenced tokens.

---

5 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

6 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

- **Notification Requirements:** Credit institutions must notify the competent authority of their intent to offer or trade asset-referenced tokens, providing information that allows verification of their ability to comply with MiCA Regulation. This notification must be submitted at least 90 working days before the token is issued.

Requirements for Offering or Trading

- **Compliance with Both Regulations:** Credit institutions must adhere to all applicable requirements of both the MiCA Regulation and Directive 2013/36/EU, including those related to asset reserves, governance, risk management, and internal controls.
- **Crypto-Asset White Paper:** A white paper must be approved by the competent authority before publication.
- **Administrative Powers:** Credit institutions are subject to administrative powers under both the MiCA Regulation and Directive 2013/36/EU, including restrictions, limitations, and potential suspension or prohibition of token offerings.

Notification to the competent authority

Credit institutions must include the following in their notification:

1. **Program of Operations:** Business model details.
2. **Legal Opinion:** Confirmation that the token is not excluded from MiCA Regulation or classified as an e-money token.
3. **Governance Description:** Organisational structure, risk management, and internal controls.
4. **Policies and Procedures:** Information on asset reserves, custody, rights granted, issuance and redemption mechanisms, transaction validation, and liquidity management.
5. **Third-Party Contracts:** Documentation of roles and responsibilities if third parties are involved in asset operations.
6. **Business Continuity Policy:** Plans to ensure data and operational continuity.
7. **Internal Controls and Risk Management:** Controls for managing ICT systems and third-party dependencies.
8. **Data Safeguarding:** Systems to protect data integrity and confidentiality.

Assessment of the notification by the competent authority

- **Authority's Assessment:** The competent authority has 20 working days to assess the completeness of the notification. If incomplete, the authority

will request missing information and set a 20-day deadline for its provision, suspending the 90-day notification period during this time. Additional requests for information will not affect the 90-day period.

- **Offering and Trading:** The asset-referenced token cannot be offered to the public or traded until the notification is complete and approved.
- **Updated Information:** For subsequent issuances, credit institutions must confirm that any previously submitted information remains accurate but are not required to resubmit unchanged details.

2. Crypto-asset white paper for the asset-referenced tokens

Issuers seeking to offer or trade asset-referenced tokens must create a detailed crypto-asset white paper, which is essential for obtaining approval from the competent authority in their home Member State.

2.1. Content and Form of the White Paper

The white paper must be comprehensive, clear, and free from material omissions. It should cover the following key areas:

- Issuer Information: Details about the entity issuing the token.
- Token Information: A thorough description of the asset-referenced token.
- Offer and Trading Information: Specifics about the public offering or admission to trading of the token.
- Rights and Obligations: Explanation of the rights and obligations associated with the token.
- Technology Information: Overview of the underlying technology used in the token.
- Risk Information: A detailed account of the risks involved with the token.
- Asset Reserve Details: Information on the assets that back the token.
- Environmental Impact: Disclosure of the environmental impact of the consensus mechanism used for the token.

If someone other than the issuer prepares the white paper, it must include the identity of that person and the reason for their involvement.

2.2. Risk and Limitation Statements

The white paper must explicitly outline potential risks, ensuring transparency about the token's financial and operational aspects. It must clearly state:

- The possibility of losing value, either partially or fully.
- Potential challenges with token transferability and liquidity.
- There is a lack of protection under investor compensation schemes or deposit guarantee schemes.

The issuer's management must provide a statement confirming that the white paper is compliant with regulations and that the information provided is accurate, clear, and not misleading.

2.3. Summary of Key Information

Following the management statement, the white paper should include a succinct summary that presents an easy-to-understand overview of the token offering or trading details. This summary should caution readers that it is only an introduction, advising them to base their decisions on the full white paper. It should also clarify that the white paper is not a financial prospectus.

2.4. Language and Form Requirements

The white paper must be written in the official language of the issuer's home Member State or in a language commonly used in international finance. If the token is offered in another Member State, the white paper should also be provided in the official language of that State or a commonly used financial language. Additionally, the document must avoid speculative statements about future token value, include the publication date and a table of contents, and be available in a machine-readable format.

This structured approach ensures that all relevant information is provided, facilitating informed decision-making by potential investors while maintaining compliance with regulatory standards.

2.5. Publication of the Crypto-Asset White Paper

The issuer of an asset-referenced token must publish the approved crypto-asset white paper and, if applicable, any modified versions on their website. This publication must be accessible to the public from the start of the offer or admission to trading of the token and must remain available until the token is no longer held by the public.

2.6. Liability of Issuers of Asset-Referenced Tokens for the Information Given in a Crypto-Asset White Paper

Liability for Non-Compliance

Issuers are liable for any losses incurred by token holders if they fail to comply with MiCAR requirements concerning the content and form of the crypto-asset white paper. This includes providing incomplete, misleading, or unclear information. Any attempt to exclude or limit civil liability in such cases is void.

Burden of Proof

Token holders must provide evidence that the issuer's white paper, or a modified version, did not comply with MiCAR requirements and that this non-compliance influenced their decision to purchase, sell, or exchange the asset-referenced token.

Liability Limitation

Issuers and their administrators are not liable for losses caused by reliance on information in a summary unless the summary is misleading or inaccurate when read in conjunction with the rest of the white paper or fails to provide essential information for decision-making.

2.7. Modification of Published Crypto-Asset White Papers for Asset-Referenced Tokens

Notification of Changes

Issuers must inform the competent authority in their home Member State about any material changes to their business model that could affect token holders' decisions. This includes modifications to governance arrangements, reserve assets, token rights, issuance mechanisms, transaction protocols, distributed ledger technology, liquidity management, third-party arrangements, complaints handling procedures, and risk assessments related to money laundering and terrorist financing. Notifications must be made at least 30 days before changes take effect.

Decision by the Competent Authority

Upon receiving notice of proposed changes, issuers must submit a draft of the modified crypto-asset white paper.

The competent authority will review this draft and make a decision within 30 days, with the possibility of an extension if additional information is requested. The authority may require protective measures or corrective actions if the modifications could impact market integrity, financial stability, or payment systems.

Informing Supervisory Authorities

For changes affecting payment systems, monetary policy, or sovereignty, the competent authority must consult the ECB, national central banks, and other relevant bodies. The ECB, central banks, EBA, and ESMA must provide their opinions within 20 days. The authority must then implement the recommended corrective measures. If the ECB or central bank proposes different measures, these must be combined or stricter measures applied.

Publication of Modified White Paper

After approval, the competent authority must send the modified white paper to ESMA, the host Member State's contact, and the central bank within two days. ESMA will then add the modified white paper to its register.

2.8. Development of Implementing and Regulatory Technical Standards

ESMA and EBA are tasked with creating draft standards for forms, formats, and templates related to the crypto-asset white paper. These standards can be adopted by the Commission under Article 15 of Regulation (EU) No 1095/2010[7].

Draft Standards on Sustainability Indicators

ESMA and EBA will also develop draft standards on sustainability indicators, including the environmental impacts of consensus mechanisms.

3. Overview of obligations of issuers of asset-referenced tokens

3.1. Obligation to Act Honestly, Fairly, and Professionally in the Best Interest of Token Holders

Issuers must act with honesty and fairness, ensuring that all communications are clear and non-misleading.

---

7 Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC.

They must prioritise the interests of token holders and treat them equally unless preferential treatment is disclosed in the white paper and marketing materials.

3.2. Marketing Communications

Marketing Communications Requirements
Marketing communications must be identifiable, fair, clear, and consistent with the white paper. They should indicate that a white paper is available and provide issuer contact details. Marketing communications must also state that token holders have redemption rights.

Availability of Marketing Communication
Marketing communications should be published on the issuer's website without prior approval and made available to authorities if requested. They cannot be distributed before the white paper is published, but market soundings are allowed.

3.3. Ongoing Information to Holders of Asset-Referenced Tokens

Information Requirements
Issuers must disclose and update the amount of tokens in circulation, the reserve assets' value and composition, and any significant events affecting these. This information, including an audit report summary, must be updated monthly and posted on the issuer's website.

3.4. Reporting on Asset-Referenced Tokens

Obligations of the Competent Authority
For tokens with an issue value above EUR 100 million, issuers must report quarterly on the number of holders, token value, reserve size, transaction averages, and token use as a means of exchange. The competent authority may require reporting for tokens below this threshold and share information with the ECB, central banks, and host Member States.

Obligations of Crypto-Asset Service Providers
Service providers must supply issuers with the necessary information for reporting, including transactions outside the distributed ledger.

Obligations of the ECB
The ECB and central banks may provide their own transaction estimates to the competent authority.

Development of Technical Standards
The EBA, in collaboration with the ECB, will develop draft regulatory and implementing technical standards for estimating and reporting transactions associated with asset-referenced tokens. These standards are adopted by the Commission under Regulation (EU) No 1093/2010 [8].

3.5. Restrictions on the Issuance of Asset-Referenced Tokens Used Widely as a Means of Exchange

Issuance Restrictions
If an asset-referenced token has an estimated daily transaction volume of over 1 million and a value exceeding EUR 200 million, the issuer must:

- Cease issuing the token.
- Submit a plan within 40 days to the authority to reduce transactions below 1 million and the value below EUR 200 million.

Assessment of Compliance
The competent authority will assess compliance using data provided by the issuer, its own estimates, or those from the ECB or central bank, whichever is higher. For multiple issuers of the same token, data from all issuers will be aggregated.

Approval of the Plan
The plan to reduce transactions and value must be approved by the competent authority, which may require modifications such as imposing a minimum denomination to ensure compliance.

Re-Issuance
The token may only be re-issued when evidence shows that the estimated quarterly average number of transactions and value are below the specified thresholds.

3.6. Obligation to Have a Reserve of Assets and Composition and Management of Such Reserve

Reserve Requirements
Issuers must maintain a reserve of assets that:

- Covers risks associated with the assets referenced by the tokens.

---

8 Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC.

- Addresses liquidity risks related to token redemption rights. The reserve must be kept separate from the issuer's other assets and from other tokens to protect token holders and prevent creditors from accessing the reserve in case of bankruptcy.

Separate Pools for Multiple Tokens
Issuers with multiple asset-referenced tokens must maintain separate asset pools for each token. If different issuers offer the same token, only one pool of assets is required.

Management and Valuation
The reserve must be effectively managed to ensure that token issuance and redemption align with the reserve's value. The value of the reserve must match or exceed the value of claims from token holders.

EBA Draft Standards
The EBA developed draft regulatory technical standards for liquidity requirements, including reserve percentages, minimum deposits, and liquidity management techniques.

Custody of Reserve Assets

Custodial Requirements
Issuers must ensure that:

- Reserve assets are not pledged as collateral.
- Assets are held in custody and accessible quickly for redemption requests.
- Custodians are not concentrated, and assets are not concentrated.

Custody Policy
Each pool of reserve assets must have a dedicated custody policy. If multiple issuers manage the same token, they must share a single custody policy.

Asset Management
Reserve assets must be held in custody within five working days of issuance. Custodians can be crypto-asset service providers, credit institutions, or investment firms, with contracts protecting reserve assets from custodians' creditors.

Contractual Obligations
Custodians must be appointed via contracts outlining their roles, responsibilities, and legal jurisdiction. Custodians must act honestly, fairly, and independently, avoiding conflicts of interest. Contracts must also address how conflicts of interest are managed and disclosed.

Liability

If reserve assets are lost, custodians must replace them with identical or equivalent assets, except when loss is due to external events beyond their control.

Investment of the Reserve of Assets

Investment Requirements for Issuers

- Investment Criteria: Issuers must invest the reserve of assets in highly liquid, low-risk financial instruments that can be quickly liquidated with minimal price impact.
- UCITS: Units in a UCITS are deemed low-risk if the UCITS invests according to EBA guidelines and minimises concentration risk.
-

Profit and Loss Responsibility

- Issuer Liability: Issuers are responsible for all profits and losses from the investment of reserve assets, including value fluctuations and risks from counterparties or operations.

Development of Standards by Regulatory Bodies

(a) Liquidity Requirements

- Draft Standards: The EBA, with ESMA and the ECB, will draft standards defining highly liquid, low-risk financial instruments. These standards will include:
  - Types of Assets: Guidelines on asset types that can be referenced by asset-referenced tokens.
  - Liquidity Coverage: Requirements for holding sufficient liquid assets to cover shortfalls for at least 30 days, with specific rules on inflow and outflow management.
  - Concentration Constraints: Limits on how much can be invested in instruments from a single entity and holding crypto-assets with a single group.

b) Concentration Requirements

- UCITS Investment Limits:
  - Securities/Money Market Instruments: No more than 5% of assets in instruments from the same issuer or 20% in deposits with the same body.
  - Counterparty Exposure: Limits of 10% for credit institutions and 5% for others.
  - Aggregate Limits: Member States can raise the 5% limit to 10%, but total investments in issuing bodies cannot exceed 40% of assets.

- Combination Constraints: UCITS cannot exceed 20% of assets in a single body when combining securities, deposits, or OTC derivatives.
- Regulatory Timeline: The EBA submitted draft technical standards. The Commission may supplement these regulations as per Articles 10 to 14 of Regulation (EU) No 1093/2010.

Right of Redemption

- **Right to Redeem:** Holders can request redemption at any time if the issuer fails to meet obligations. Issuers must provide a clear policy on redemption.
- **Redemption Terms:** Issuers must pay either the market value or deliver the assets. The redemption policy must include:
  - **Conditions:** Terms for exercising the right of redemption.
  - **Procedures:** Mechanisms for redemption, including during market stress, and details on recovery and redemption plans.
  - **Valuation:** Use of mark-to-market valuation for assets, ensuring accuracy and quality of market data.
  - **Settlement:** How redemption is settled and how issuers manage reserve asset changes to avoid market impact.
- **Currency:** If payments are accepted in non-electronic money, redemption must be offered in the same currency.
- **Fees:** No redemption fees are allowed for asset-referenced tokens.

3.7. Prohibition of granting interest

- Issuers and crypto-asset service providers are prohibited from giving interest on asset-referenced tokens.
- Any financial benefit related to the duration of holding these tokens, such as compensation or discounts, is considered interest and is disallowed.

3.8. Maintaining recovery and redemption plans

Recovery plan

- Issuers must create a recovery plan to address potential issues with asset-referenced tokens, ensuring continued operation and compliance with obligations during disruptions.
- The plan should include measures like liquidity fees, redemption limits, and possible suspension of redemptions.
- Issuers must submit the plan to relevant authorities within six months of authorisation or approval, with regular updates and amendments as needed.

- Competent authorities have the power to enforce recovery measures or suspend redemptions to protect token holders and financial stability.

Redemption plan

- Issuers must also create a redemption plan for orderly token redemptions in case they cannot meet their obligations due to insolvency or withdrawal of authorisation.
- This plan ensures timely payment to token holders and prevents market instability, with provisions for appointing a temporary administrator if necessary.
- The issuer must notify relevant authorities of the redemption plan within six months of authorisation, with updates and amendments as required.

4. Significant asset-referenced tokens

4.1. Classification of Significant Asset-Referenced Tokens

Criteria for Classification

An asset-referenced token is classified as significant if it meets at least three of the following criteria:

- **Holder Count:** More than 10 million holders.
- **Market Capitalization/Reserve:** Over EUR 5 billion.
- **Transaction Volume:** More than 2.5 million daily transactions and EUR 500,000 in daily transaction value.
- **Issuer Type:** Issued by a gatekeeper platform.
- **International Use:** Significant use for international payments.
- **Financial System Connection:** Strong connection to the financial system.
- **Issuer Activity:** The issuer issues other tokens or provides crypto-asset services.

Reporting

- Frequency: Member States must report to the EBA and ECB twice a year on whether tokens meet the significant classification criteria.

Classification Process

- Draft Decision: If the EBA identifies a token as significant, it issues a draft decision and seeks input from issuers, the ECB, and national authorities.

- Response Period: Relevant parties have 20 days to respond before the EBA makes a final decision.

Annual Review

- Review Process: The EBA reviews the classification annually. If a token no longer meets the criteria, the EBA will draft a decision to remove its significant status, considering input before making a final decision.

Final Decision

- Timeline: The EBA finalises classification decisions within 60 days and notifies relevant parties.

Transfer of Responsibilities

- Oversight Shift: Once classified as significant, oversight shifts from national authorities to the EBA. If the token loses its significant status, oversight transfers back to national authorities.

Delegated Acts

- Further Rules: The Commission will adopt additional rules specifying criteria for international significance, connection to the financial system, and reporting requirements.

4.2. Voluntary Classification of Asset-Referenced Tokens as Significant

Application for Voluntary Classification

- Issuers of asset-referenced tokens can request that their tokens be classified as significant during their application for authorisation.
- Upon receiving such a request, the authority must inform the EBA, ECB, and, when relevant, the central bank of the concerned Member State.

Draft Decision Process

- **Timeline**: The EBA must prepare a draft decision within 20 days of receiving the request, assessing whether the token meets the criteria.
- **Consultation**: The draft is shared with the issuer's home Member State authority, the ECB, and relevant central banks, who have 20 working days to provide feedback.
- **Consideration**: The EBA reviews these comments before finalising its decision.

Final Decision

- **Timeline:** The EBA will make a final decision within 60 days and notify the issuer and relevant authorities.

Transfer of Supervisory Responsibilities

- If classified as significant, supervisory responsibilities for the token shift from the national authority to the EBA, effective either on the date of authorisation or approval of the crypto asset white paper.

4.3. Specific additional obligations for issuers of significant asset-referenced tokens

Issuers of significant asset-referenced tokens must adopt a remuneration policy that promotes sound risk management, avoiding incentives to lower risk standards. Tokens must be accessible to authorised providers, including those outside the issuer's group, on a fair and non-discriminatory basis.

Issuers are required to assess and monitor liquidity needs to meet redemption requests, establishing a liquidity management policy to ensure resilient reserve assets, even under stress scenarios. Regular liquidity testing is mandatory, and the EBA may require additional liquidity based on results. A minimum of 60% of deposits must be held in each referenced official currency, with a 3% reserve asset requirement for significant tokens.

These obligations apply to each issuer if multiple entities offer the same significant token. If an issuer offers multiple tokens, including at least one significant one, all obligations apply. The EBA and ESMA draft technical standards on remuneration and liquidity management policies.

See also EBA's Draft Regulatory Technical Standards to specify the minimum contents of the liquidity management policy and procedures under Article 45(7)(b) of Regulation (EU) 2023/1114.

The EBA, ESMA, and ECB will issue and regularly update stress test guidelines, considering market developments.

IV. Overview of E-Money Tokens[9]

E-money tokens are digital representations of value that are primarily used for making electronic payments and are classified as a form of electronic money under EU law. The regulation of e-money tokens within the European Union (EU) is governed by specific requirements that ensure the protection of consumers and the stability of financial markets.

1. Requirements to be fulfilled by all issuers of e-money tokens

Authorisation and Compliance

Issuers are required to be authorised as either credit institutions or electronic money institutions. They must notify the competent authorities of their intentions through a crypto-asset white paper, which must also be published. Unauthorised individuals or entities can only offer or trade e-money tokens with the issuer's written consent. They must also comply with regulations prohibiting the granting of interest and adhering to specific marketing communications guidelines.

Classification and Notification

E-money tokens are classified as electronic money, particularly when they reference the official currency of an EU Member State. Issuers are obligated to notify relevant authorities at least 40 days before making these tokens available to the public. If certain conditions apply, a white paper detailing the specifics of the tokens must also be prepared and shared with the authorities.

Legal Framework and Exemptions

The issuance and use of e-money tokens are primarily governed by Titles II and III of Directive 2009/110/EC[10], which outline the legal framework for electronic money institutions. However, certain exemptions apply to issuers under specific articles of the Directive, allowing for limited deviations from these regulations.

---

9 Title IV, Articles 48 to 58, Annex III, and Annex VI contain the provisions on E-money tokens in the Markets in Crypto-assets (MiCA) Regulation.

10 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

Issuance and Redeemability

E-money tokens must be issued at par value upon receipt of funds and can be redeemed by holders at any time, also at par value. Importantly, no fees can be charged for redemption. The issuer's obligations and the rights of the token holders must be clearly stated in the crypto-asset white paper, ensuring transparency and accountability.

Prohibition of Interest

Both issuers and crypto-asset service providers are strictly prohibited from granting interest on e-money tokens. This prohibition extends to any benefits or compensations that could be interpreted as interest, including discounts or other forms of compensation tied to the duration of holding the tokens.

2. Crypto-Asset White Paper Requirements

Content and Form Requirements

The white paper must provide comprehensive information in several key areas:

1. Issuer Details: This includes the legal and commercial information of the entity issuing the e-money token.
2. Token Description: A clear explanation of the token's characteristics, functionalities, and underlying technology.
3. Offer Details: Information on the public offering or admission of the token to trading, ensuring transparency in its distribution.
4. Rights and Obligations: A detailed description of the rights and obligations associated with holding the token.
5. Risk Factors: Disclosure of risks, including potential adverse impacts on climate and the environment.
6. Compliance Statements: The document must include statements from the issuer's management affirming the accuracy and completeness of the white paper.

The white paper must be clear, concise, and devoid of misleading information. It should also include specific warnings about the lack of coverage by investor compensation and deposit guarantee schemes.

Publication and Notification

Before offering e-money tokens to the public or seeking their admission to trading, issuers must publish the white paper on their website and notify the

elevant regulatory authorities at least 20 days in advance. Any subsequent modifications due to errors or new information must also be updated and notified. This ensures that all stakeholders have access to current and accurate information.

Regulatory Standards and Liability

The European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA) developed technical standards for the forms and templates used in these white papers. Issuers are held liable for any losses incurred by token holders if the white paper contains misleading or incomplete information. This liability extends to the issuer's administrative, management, or supervisory body. However, liability does not generally extend to summaries unless they are misleading or omit key information.

See also ESMA's Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA) – second consultation paper.

3. Marketing Communications

Marketing communications concerning e-money tokens must be clearly identifiable, fair, clear, and consistent with the information provided in the white paper. These communications must inform potential investors about the right of redemption and cannot be disseminated before the white paper's publication.

4. Investment and Safeguarding of Funds

Issuers are required to deposit at least 30% of funds in separate accounts in credit institutions, while the remainder should be invested in secure, low-risk financial instruments. These measures ensure the stability and security of the funds backing the e-money tokens.

5. Recovery and Redemption Plans

Issuers of e-money tokens are required to maintain comprehensive recovery and redemption plans. These plans should address operational failures or instances of non-compliance, detailing strategies to restore operations and fulfil obligations to token holders under adverse conditions.

6. Significant E-Money Tokens

Significant e-money tokens are subject to additional regulatory scrutiny.

The classification process takes into account the scale of issuance and market impact, among other criteria.

(a) Classification Criteria
E-money tokens are classified as "significant" by the EBA if they meet at least three of the following criteria used for asset-referenced tokens:

- **Number of Holders:** More than 10 million holders.
- **Market Value:** Market capitalisation or reserve assets exceed EUR 5 billion.
- **Transaction Volume:** Daily transactions exceed 2.5 million and EUR 500,000 in value.
- **Core Platform Services:** Issued by a provider designated as a gatekeeper under EU regulations.
- **International Significance:** Used widely for payments and remittances on an international scale.
- **Financial System Connectivity:** Strong links with the financial system.
- **Issuer Activity:** The issuer also issues other tokens or provides crypto-asset services.

These criteria must be met either during the first reporting period after the public offering or during two consecutive reporting periods. If multiple issuers are involved, their data is aggregated.

(b) Reporting and Classification Process
Issuers' home Member State authorities must report biannually to the EBA and European Central Bank (ECB) on whether the criteria are being met, covering aspects like the number of holders, transaction volumes, and asset reserves. If the token is issued in a non-euro country, the information is also sent to that country's central bank.

If the EBA identifies that a token meets the significance criteria, it will draft a decision to classify it as significant and consult with relevant authorities before finalising the decision within 60 days. The decision can be revisited annually, and if a token no longer meets the criteria, the EBA may declassify it as significant.

c) Transfer of Supervisory Responsibilities
Once a token is classified as significant, supervisory responsibilities are transferred from the national competent authority to the EBA within 20 days. If the token is declassified, these responsibilities revert to the national authority. However, if 80% of the token's transactions occur within one Member State, supervisory duties remain with the national authority.

(d) Voluntary Classification

Issuers can voluntarily request their e-money tokens be classified as significant by demonstrating they meet at least three of the criteria. The EBA then follows a similar process to the mandatory classification, involving consultation and a final decision within 60 days.

(e) Additional Obligations for Significant Tokens

Issuers of significant e-money tokens must adhere to stricter requirements:

- Asset Reserve: Maintain and manage a reserve of assets with specific guidelines for custody and investment.
- Risk Management: Implement a remuneration policy that promotes effective risk management and prevents risky behaviour.
- Liquidity Management: Develop a liquidity management policy, conduct regular liquidity tests, and ensure adequate deposits in each referenced currency.
- Capital Requirements: Maintain higher reserve assets and own funds.

These obligations replace certain requirements from Directive 2009/110/EC[11]. Additionally, significant tokens must undergo an independent audit every six months, and Member States may impose additional requirements to address specific risks. For tokens denominated in non-EU currencies, specific rules on reporting, issuance restrictions, and authorisation withdrawal apply.

11 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amendingDirectives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

V. Authorisation of Crypto-Asset Service Providers[12]

Crypto-Asset Services is any of the following services and activities relating to any crypto-asset:

- providing custody and administration of crypto-assets on behalf of clients;
- operation of a trading platform for crypto-assets;
- exchange of crypto-assets for funds;
- exchange of crypto-assets for other crypto-assets;
- execution of orders for crypto-assets on behalf of clients;
- placing of crypto-assets;
- reception and transmission of orders for crypto-assets on behalf of clients;
- providing advice on crypto-assets;
- providing portfolio management on crypto-assets;
- providing transfer services for crypto-assets on behalf of clients.

Crypto-Asset Service Providers (CASPs) are legal persons or other undertakings whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis and that are allowed to provide crypto-asset services.

The regulation applies to individuals, companies, and other entities that issue, offer, or facilitate crypto-assets trading or provide services related to crypto-assets within the EU.

Exemptions from the Regulation

The regulation does not apply to:

- Entities offering crypto-asset services exclusively to their parent companies;
- Subsidiaries or other subsidiaries of the same parent company;
- Liquidators or administrators acting during insolvency procedures;

The European Central Bank (ECB), EU member states' central banks acting in their monetary authority capacity, or other public authorities;

12 The provisions on Crypto-Asset Service Providers in the Markets in Crypto-assets (MiCA) Regulation are contained in Title V, Articles 59 to 85 and Annex II and Annex IV.

- The European Investment Bank and its subsidiaries, the European Financial Stability Facility, and the European Stability Mechanism;
- Public international organisations;
- Unique and non-fungible crypto-assets are exempt.

Crypto-Assets Excluded from the Regulation:

- Financial instruments;
- Deposits (including structured deposits);
- Funds, unless they are classified as e-money tokens;
- Securitisation positions as defined in EU regulations;
- Non-life or life insurance products, reinsurance, and retrocession contracts;
- Pension products intended to provide retirement income;
- Officially recognised occupational pension schemes;
- Individual pension products requiring employer contributions under national law;
- Pan-European Personal Pension Products (PEPP);
- Social security schemes covered by EU regulations.

Authorisation of crypto-asset service providers

1. Authorisation

Requirement for Authorisation

To provide crypto-asset services within the Union, an entity must be:

- (a) A legal entity or other undertaking authorised as a crypto-asset service provider under point 5 of this chapter (Assessment of the Application for Authorisation and Grant or Refusal of Authorisation).
- (b) A credit institution, central securities depository, investment firm, market operator, electronic money institution, UCITS management company, or alternative investment fund manager authorised to provide such services under point 2 of this chapter (Provision of Crypto-Asset Services by Certain Financial Entities).

Location and Management Requirements

Authorised crypto-asset service providers must have a registered office in a Member State and their effective management within the Union. At least one director must reside in the Union.

Non-Legal Persons as Service Providers

Non-legal entities may offer crypto-asset services if their legal form ensures equivalent rotection for third-party interests and if they are under equivalent

prudential supervision.

Ongoing Compliance
Service providers must continuously meet the conditions of their authorisation.

Misrepresentation Prohibition
Entities not authorised as crypto-asset service providers must not mislead the public by using names or marketing communications that suggest they are authorised.

Authorisation Specificity
Competent authorities must ensure that authorisations clearly specify the crypto-asset services the provider is authorised to offer.

Union-Wide Service Provision
Authorised providers may offer services across the Union, either by establishing branches or through the freedom to provide services without needing a physical presence in host Member States.

Expanding Authorised Services
To add new services, providers must request an extension from the competent authority that granted their initial authorisation and update all relevant information.

2. Provision of Crypto-Asset Services by Certain Financial Entities

Credit Institutions
A credit institution may provide crypto-asset services if it notifies its home Member State's authority at least 40 working days before starting the services.

Central Securities Depositories
Central securities depositories may provide custody and administration of crypto-assets if they notify their home authority at least 40 days in advance.

Investment Firms
Investment firms may offer crypto-asset services equivalent to those already authorised under Directive 2014/65/EU[13], with prior notification to the home authority.

---

13 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

Electronic Money Institution
These institutions may provide crypto-asset custody and transfer services related to the e-money tokens they issue, provided they notify their home authority 40 days before starting.

UCITS and AIF Managers
These entities may provide crypto-asset services equivalent to their authorised investment and management activities if they notify their home authority 40 days in advance.

Market Operators
Market operators authorised under Directive 2014/65/EU may operate trading platforms for crypto-assets with prior notification.

Notification Requirements
Entities must notify their home authority with specific information, including operational plans, compliance mechanisms, risk management frameworks, ICT systems documentation, and segregation policies for client assets.

Authority Review Process
Upon receiving a notification, the authority has 20 days to assess completeness. If incomplete, the authority must inform the entity and set a deadline for providing missing information, suspending the service start date until complete.

Avoiding Duplicate Submissions
Entities need not resubmit identical information already provided to the authority, provided they confirm that the previously submitted information remains up-to-date.

Revocation of Service Rights
The right to provide crypto-asset services is revoked if the relevant authorisation is withdrawn.

ESMA Communication
Competent authorities must communicate the required information to ESMA after verifying its completeness, which ESMA will include in the relevant register.

Development of Regulatory Standards
The European Securities and Markets Authority (ESMA), in cooperation with the European Banking Authority (EBA), has developed draft regulatory technical standards that specify the information required in the notification

process. These drafts were submitted to the Commission, which was empowered to adopt them.

Development of Implementing Technical Standards
ESMA and the EBA have also developed a draft implementing technical standards to establish standard forms, templates, and procedures for the notification process.

3. Provision of Crypto-Asset Services at the Exclusive Initiative of the Client (also known as Reverse Solicitation)

Client-Initiated Services

This is considered a reverse solicitation when a client established or situated in the Union initiates a crypto-asset service or activity on their own exclusive initiative with a third-country firm. In such cases, the requirement for authorisation does not apply. This exemption also covers any relationship specifically related to the provision of that crypto-asset service or activity.

However, if the third-country firm solicits clients or prospective clients within the Union—whether through any entity acting on its behalf, close links, or any other person acting on its behalf—such services will not be deemed initiated by the client. This holds true regardless of the means of communication used and supersedes any contractual clause or disclaimer.

Limitations on Client-Initiated Services

A third-country firm cannot market new types of crypto-assets or services to the client under the premise of the client's exclusive initiative.
ESMA Guidelines

By December 30, 2024, ESMA will issue guidelines under Article 16 of Regulation (EU) No 1095/2010[14] to specify situations where a third-country firm is deemed to solicit clients in the Union. These guidelines will also address supervision practices to prevent abuse and circumvention of this regulation[15].

---

14 Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC.

15 EUCI response to the ESMA's guidelines under Article 16 of Regulation (EU) No 1095/2010: https://docs.google.com/document/d/11482tF2MvFIZGQqOvVntEggIRmBDw5DDgvXeVytYnwg/edit#heading=h.8o713td15o8r.

4. Application for Authorisation as a Crypto-Asset Service Provider

Submission of Application

Entities intending to provide crypto-asset services must submit an application for authorisation to the competent authority of their home Member State.

Required Information for Application

The application must include the following:

a. Name, legal entity identifier, website, contact information, and physical address.
b. Legal form of the applicant.
c. Articles of association, if applicable.
d. A program of operations detailing the types of services and marketing strategies.
e. Proof of compliance with prudential safeguards.
f. Description of governance arrangements.
g. Proof that the management body members are of good repute and possess the necessary knowledge, skills, and experience.
h. Identity and holdings of significant shareholders, along with proof of their good repute.
i. Provide a description of internal controls, risk management, and business continuity plans.
j. Technical documentation of ICT systems and security arrangements.
k. Procedure for segregating clients' crypto-assets and funds.
l. Description of complaints handling procedures.
m. Custody and administration policy, if applicable.
n. Operating rules and market abuse detection system for trading platforms, if applicable.
o. Non-discriminatory commercial policy and pricing methodology, if applicable.
p. Execution policy for orders, if applicable.
q. Proof of knowledge and expertise of persons providing advice or portfolio management.
r. Information on transfer services, if applicable.
s. Type of crypto-asset related to the service.

Proof of Good Repute

Applicants must provide evidence of the absence of criminal records or

penalties related to commercial law, insolvency law, financial services law, anti-money laundering, counter-terrorist financing, fraud, or professional liability for:

a. All members of the management body.
b. Shareholders and members with significant holdings.

Previously Submitted Information

Competent authorities cannot request information already submitted under previous authorisations if it remains up-to-date.

ESMA's Role in Regulatory Standards

ESMA, in cooperation with the EBA, has developed draft regulatory technical standards to specify the information required in paragraphs 2 and 3. These drafts were submitted to the Commission and it has the power to adopt these standards.

Development of Implementing Technical Standards

ESMA, with the EBA's cooperation, has also established standard forms, templates, and procedures for the application process. These were also submitted to the Commission and it holds the authority to adopt these standards.

5. Assessment of the Application for Authorization and Grant or Refusal of Authorisation

Acknowledgment of Application

Competent authorities must acknowledge receipt of an application for authorisation within five working days.

Completeness Check

Within 25 working days of receiving the application, competent authorities must assess whether the application is complete by verifying that all required information listed in point 4 of this chapter has been provided. If the application is incomplete, a deadline will be set for the applicant to provide the missing information.

Incomplete Applications

Authorities may refuse to review applications that remain incomplete after the set deadline.

Notification of Completeness

Once the application is complete, authorities must promptly notify the applicant.

Cross-Border Consultation

Before granting or refusing authorisation, competent authorities must consult with authorities in other Member States if the applicant is linked to entities such as credit institutions, investment firms, or other financial entities within those states.

AML and CTF Consultation

Authorities may consult anti-money laundering (AML) and counter-terrorist financing (CTF) authorities to ensure the applicant has not been involved in such activities. Compliance with relevant AML/CTF laws must also be verified, especially for operations in high-risk countries.

Close Links Evaluation

Authorisation will only be granted if close links between the applicant and other entities do not hinder effective supervision.

Third-Country Links

Authorisation will be refused if laws or regulations in the third country, governing entities with close links to the applicant, prevent effective supervision.

Final Assessment and Decision

Authorities have 40 working days from the receipt of a complete application to assess whether the applicant complies with all relevant regulations. A fully reasoned decision to grant or refuse authorisation must be made and communicated to the applicant within five working days.

Grounds for Refusal

Authorisation will be refused if:

- The management body poses a threat to effective management, market integrity, or AML/CTF compliance.
- The management body or significant shareholders do not meet the criteria for good repute.
- The applicant is likely to fail to meet regulatory requirements.

Guidelines on Suitability

ESMA and EBA jointly issued guidelines on assessing the suitability of management and significant shareholders.

Requests for Additional Information

Authorities may request further information during the assessment period, suspending the assessment period until the information is received. The suspension period cannot exceed 20 working days.

Communication with ESMA

Authorities must communicate authorisation decisions to ESMA within two working days. ESMA will update the relevant register with this information.

6. Withdrawal of Authorization of a Crypto-Asset Service Provider

Mandatory Withdrawal

Authorities must withdraw authorisation if the crypto-asset service provider:

- Fails to use its authorisation within 12 months.
- Renounces its authorisation.
- Stops providing services for nine consecutive months.
- Obtained authorisation through irregular means.
- No longer meets the conditions for authorisation and fails to take remedial action.
- Fails to prevent money laundering or terrorist financing.
- It seriously infringes regulations protecting clients or market integrity.

Discretionary Withdrawal

Authorities may withdraw authorisation if the provider:

- Violates AML/CTF regulations.
- Loses authorisation as a payment or electronic money institution and fails to remedy the situation within 40 days.

Notification to ESMA

Upon withdrawing authorisation, authorities must notify ESMA and relevant host Member States. ESMA will update the register accordingly.

Partial Withdrawal

Authorities may limit the withdrawal to specific services offered by the provider.

Cross-Border Consultation

Before withdrawing authorisation, authorities must consult with relevant authorities in other Member States if the provider is connected to entities in those states.

AML/CTF Consultation

Authorities may also consult AML/CTF authorities before withdrawing authorisation.

Requests for Compliance Review

EBA, ESMA, or any host Member State authority may request a review to ensure the provider still meets authorisation conditions.

Client Asset Transfer

Providers must have procedures in place to ensure the timely and orderly transfer of client assets to another provider if authorisation is withdrawn.

7. Cross-Border Provision of Crypto-Asset Services (Passportisation)

Submission of Information

Crypto-asset service providers intending to offer services in multiple Member States must submit the following information to their home Member State's competent authority:

- A list of Member States where services will be provided.
- The specific crypto-asset services that are to be offered on a cross-border basis.
- The intended start date for providing these services.
- A list of any other activities conducted by the provider not covered by this regulation.

Communication by Competent Authority

The competent authority of the home Member State must communicate the information to the single points of contact in the host Member States, ESMA, and EBA within 10 working days of receiving it.

Notification to Service Provider

The home Member State's competent authority must promptly inform the crypto-asset service provider of the communication made to the relevant authorities.

Commencement of Services

The crypto-asset service provider may begin offering services in other Member States either upon receipt of the communication from the competent authority or no later than 15 calendar days after submitting the required information.

Acquisition of crypto-asset service providers

1. Assessment of Proposed Acquisitions of Crypto-Asset Service Providers

Notification Requirements

- **Acquisition Notification:**
  - Who Must Notify: Any natural or legal person (or persons acting in concert) intending to acquire or increase their qualifying holding in a

a crypto-asset service provider.

a. Thresholds: Notifications are required if the holding reaches or exceeds 20%, 30%, or 50% or if the provider becomes a subsidiary.
b. Information Required: The size of the intended holding and additional information must be included per regulatory technical standards.

- **Disposition Notification**:
  c. Who Must Notify: Any natural or legal person planning to dispose of a qualifying holding or reduce it below 10%, 20%, 30%, or 50%.
  d. Details: Notification must include the size of the holding being disposed of or reduced.

Authority's Actions

- **Acknowledgement of Receipt:**
  a. The competent authority must acknowledge receipt of notifications in writing within two working days.
- **Assessment Period:**
  b. Timeline: The authority must assess the proposed acquisition within 60 working days from the acknowledgement date.
  c. Notification of Expiry: The authority will inform the acquirer of the assessment period's expiry date.
- **Consultation:**
  d. The authority may consult anti-money laundering, counter-terrorist financing authorities, and financial intelligence units during the assessment.
- **Additional Information Requests:**
  e. Timing: Requests for additional information can be made before finalising the assessment, no later than the 50th working day from acknowledgement.
  f. Suspension: The assessment period is suspended until the additional information is received, up to 20 working days. Extensions of up to 30 working days are possible if the acquirer is outside the Union.
- **Opposition Notification:**
  - If the authority opposes the acquisition, it must notify the acquirer within two working days before the assessment period expires, providing reasons for the decision.
- **Deemed Approval:**
  - If no opposition is communicated by the end of the assessment period (extended if applicable), the acquisition is deemed approved.
- **Maximum Period:**
  - The competent authority may set and extend a maximum period for concluding the proposed acquisition.

2. Content of the Assessment of Proposed Acquisitions

Assessment Criteria:

- **Suitability of the Acquirer:** Reputation, knowledge, skills, and experience.
- **Financial Soundness:** Evaluates the acquirer's financial stability in relation to the business.
- Compliance: Ability of the crypto-asset service provider to meet regulatory requirements.
- **Risk of Financial Crime:** Assessment of potential money laundering or terrorist financing risks.

Opposition Grounds

The authority may oppose the acquisition based on the criteria above or if the provided information is incomplete or false.

Market Needs

Member States cannot impose conditions based on market needs or the level of qualifying holding required.

Regulatory Technical Standards:

- Development: ESMA, in cooperation with EBA, will develop detailed content requirements for assessment.
- Submission: Draft standards were submitted to the Commission.
- Delegation of Power: The Commission is authorised to adopt these standards following the procedures in Regulation (EU) No 1095/2010[16].

Significant crypto-asset service providers

1. Identification of Significant Crypto-Asset Service Providers

Criteria for Significance

A crypto-asset service provider is considered significant if it has at least 15 million active users in the Union, calculated as the average number of daily active users over the previous calendar year.

---

16 Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC.

Notification to Competent Authorities:

Timeline: Providers must notify their competent authorities within two months of reaching the 15 million active user threshold.
Authority's Role: Upon confirmation of the threshold, the competent authority must notify ESMA.

Reporting and Updates

- **Annual Updates to ESMA:**
  a. **Content:** Competent authorities of the home Member States must provide ESMA's Board of Supervisors with annual updates on:
     i. Ongoing or concluded authorisations.
     ii. Ongoing or concluded withdrawal processes.
     iii. Exercise of supervisory powers.
  b. **Additional Updates:** The competent authority may also provide more frequent updates or notify ESMA prior to decisions on authorisations or withdrawals.
- **Exchange of Views:**
  c. Updates may be followed by an exchange of views at ESMA's Board of Supervisors.

VI. Token Issuance and Public Offerings[17]

According to MiCA, an 'offer to the public' means communication to persons in any form and by any means, presenting sufficient information on the terms of the offer and the crypto-assets to be offered to enable prospective holders to decide whether to purchase those crypto-assets.

'Offeror' means a natural or legal person, another undertaking, or the issuer who offers crypto-assets to the public.

1. Offers to the Public of Crypto-Assets Other Than Asset-Referenced Tokens or E-Money Tokens

General Requirements for Public Offers

A person must meet the following conditions to offer a crypto-asset to the public in the Union:

- Should be a legal person
- Draw up a crypto-asset white paper[18]
- Notify the white paper[19]
- Publish the white paper[20]
- Draft and publish marketing communications if applicable[21]
- Comply with offeror requirements[22].

Exemptions from Certain Requirements

Certain public offers of crypto-assets are exempt from the white paper and marketing communication requirements:

- Offers to fewer than 150 persons per Member State;
- Offers with a total consideration of less than EUR 1,000,000 over 12 months;

---

17 Title II, Articles 4 to 15, and Annex I contain the provisions on token issuance and public offerings in the markets in crypto-assets (MiCA) Regulation.

18 Article 6 of MiCA

19 Article 8 of MiCA

20 Article 9 of MiCA

21 Articles 7 and 9 of MiCA

22 Article 14 of MiCA

- Offers are exclusive to qualified investors who can only hold the crypto-asset.

Further Exemptions

This Title does not apply to the following:

- Free crypto-assets;
- Crypto-assets, created as rewards for maintaining a distributed ledger;
- Utility tokens providing access to existing or operational goods or services;
- Crypto-assets used in limited networks of merchants.

If the total consideration exceeds EUR 1,000,000 in 12 months for limited network offers, the offeror must notify the competent authority. The authority may decide if the offer qualifies for an exemption.

Exemption Limitations

Exemptions do not apply if the offeror seeks to admit the crypto-asset to trading.

Service Provider Authorisation Exemption

Authorisation as a crypto-asset service provider is not required for custody, administration, or transfer services of exempt crypto-assets unless:

- Another offer of the same crypto-asset exists that is not exempt;
- The crypto-asset is admitted to a trading platform.

Utility Token Time Limit

If a public offer involves a utility token for future goods or services, the offer cannot exceed 12 months from the white paper's publication.

Subsequent Offers

Subsequent offers are treated as new offers, with exemptions possibly applying. No new white paper is required if the original one was published and consented for use.

Voluntary White Paper Publication

If an exempt offer voluntarily publishes a white paper, all regulations under this Title apply.

---

2. Admission to Trading of Crypto-Assets Other Than Asset-Referenced Tokens or E-Money Tokens

Requirements for Admission to Trading

A person must meet the following conditions to seek admission of a crypto-asset to trading within the Union:

- Should be a legal person;
- Draw up a crypto-asset white paper [23]
- Notify the white paper [24]
- Publish the white paper [25]
- Draft and publish marketing communications if applicable [26]
- Comply with offeror requirements [27].

Admission by Trading Platform Operators

If a trading platform operator admits a crypto-asset to trading without a white paper being published, the operator must fulfil all the requirements listed above.

Agreement Between Person and Platform Operator

The person seeking admission to trading and the trading platform operator can agree in writing that the operator will handle the requirements. The person must provide the platform with all necessary information for compliance.

Exemptions

Requirements to notify and publish a white paper do not apply if:

- The crypto-asset is already admitted to trading on another platform within the Union
- The white paper complies with point 3 (Content and Form of the Crypto-Asset White Paper), is updated, and consent is provided for its use in writing.

---

23 Article 6 of MiCA
24 Article 8 of MiCA
25 Article 9 of MiCA
26 Articles 7 and 9 of MiCA
27 Article 14 of MiCA

3. Content and Form of the Crypto-Asset White Paper

Required Information

The crypto-asset white paper must include the following information[28]:

- Offeror or person seeking admission to trading;
- Issuer, if different from the offeror or person seeking admission to trading;
- Operator of the trading platform (if applicable);
- Details of the crypto-asset project;
- Information on the offer to the public or admission to trading;
- Information about the crypto-asset itself;
- Rights and obligations attached to the crypto-asset;
- Underlying technology;
- Risks associated with the crypto-asset;
- Principal adverse impacts on the climate or environment from the consensus mechanism used.

If the white paper is drawn up by someone not listed above, their identity and reasons for doing so must also be provided.

Accuracy and Clarity

The information must be fair, clear, not misleading, without material omissions, and presented concisely.

Required Disclaimer

On the first page, a clear statement must be included:

- "This crypto-asset white paper has not been approved by any competent authority in any Member State of the European Union. The offeror is solely responsible for the content of this white paper."
- If prepared by a different entity (e.g., trading platform operator), the statement is adjusted accordingly.

Future Value Assertions

The white paper should not assert any future value for the crypto-asset, except for required risk disclosures.

Risk Warnings

The white paper must clearly state the following risks:

28 Further detailed in Annex I

- The crypto-asset may lose value.
- It may not always be transferable or liquid.
- Utility tokens might not be exchangeable for goods/services.
- The crypto-asset is not covered by investor compensation or deposit guarantee schemes.

Management Body Statement

A statement from the offeror's or platform operator's management body confirming compliance with this Title and ensuring the accuracy and completeness of the information is required.

Summary

A non-technical summary must be provided, clearly stating key information about the offer or trading admission, alongside warnings such as:

- The summary is an introduction and should not be the sole basis for purchasing decisions;
- The offer is not a solicitation to purchase financial instruments;
- The white paper is not a prospectus.

Date and Table of Contents

The white paper must include its notification date and a table of contents.

Language Requirements

- It must be written in the official language of the home Member State or a language customary in international finance.
- If offered in other Member States, the paper must also be available in an official language of the host Member State.

Machine-Readable Format

The white paper must be available in a machine-readable format.

ESMA's Technical Standards

ESMA, in cooperation with EBA, will develop standard forms, formats, and templates for the white paper.

Regulatory Standards for Sustainability Information

ESMA and EBA will develop technical standards for sustainability indicators

on climate and environmental impacts of consensus mechanisms used, considering energy usage, waste production, and emissions.

4. Marketing Communications

Requirements for Marketing Communications
Any marketing communications related to an offer to the public or admission to trading of crypto-assets (excluding asset-referenced and e-money tokens) must meet the following conditions:

- **Identifiability:** Clearly identified as marketing communications;
- **Accuracy:** Information must be fair, clear, and not misleading;
- **Consistency:** Must align with the information in the crypto-asset white paper[29];
- **Reference to White Paper:** Must indicate that a crypto-asset white paper has been published, providing the website, contact number, and email for further inquiries;
- **Disclaimer:** Must include the following disclaimer: "This crypto-asset marketing communication has not been reviewed or approved by any competent authority in any Member State of the European Union. The offeror of the crypto-asset is solely responsible for the content of this crypto-asset marketing communication."

If prepared by a person seeking admission to trading or an operator of a trading platform, the disclaimer should be adjusted accordingly.

Prohibition on Premature Marketing

No marketing communications should be disseminated before the crypto-asset white paper is published, except in the case of market soundings.

Competent Authority's Role

The competent authority of the Member State where the communications are disseminated has the power to assess compliance. The home Member State's authority must assist as needed.

Notification of Supervisory Actions

If a host Member State uses its supervisory powers, it must notify the home Member State's authority of the offeror or trading platform operator without undue delay.

29 If required under Articles 4 or 5 of MiCA

5. Notification of the Crypto-Asset White Paper and Marketing Communications

Notification of the White Paper

Offerors, persons seeking admission to trading, or trading platform operators must notify their crypto-asset white paper to the competent authority of their national Member State.

Notification of Marketing Communications

Upon request, marketing communications must be notified to both the national and host Member State's competent authorities when addressing prospective holders.

No Prior Approval Required

Competent authorities cannot require prior approval of the crypto-asset white papers or marketing communications before publication.

Explanation Required

Notifications must include an explanation of why the crypto-asset is not considered:

- Excluded under Article 2(4) of MiCA[30];
- An e-money token;
- An asset-referenced token.

---

30 This Regulation does not apply to crypto-assets that qualify as one or more of the following: financial instruments; deposits, including structured deposits; funds, except if they qualify as e-money tokens; securitisation positions in the context of a securitisation as defined in Article 2, point (1), of Regulation (EU) 2017/2402; non-life or life insurance products falling within the classes of insurance listed in Annexes I and II to Directive 2009/138/EC of the European Parliament and of the Council (27) or reinsurance and retrocession contracts referred to in that Directive; pension products that, under national law, are recognised as having the primary purpose of providing the investor with an income in retirement and that entitle the investor to certain benefits; officially recognised occupational pension schemes falling within the scope of Directive (EU) 2016/2341 of the European Parliament and of the Council (28) or Directive 2009/138/EC; individual pension products for which a financial contribution from the employer is required by national law and where the employer or the employee has no choice as to the pension product or provider; a pan-European Personal Pension Product as defined in Article 2, point (2), of Regulation (EU) 2019/1238 of the European Parliament and of the Council (29); social security schemes covered by Regulations (EC) No 883/2004 (30) and (EC) No 987/2009 of the European Parliament and of the Council (31).

Notification Timeline

Notification of the white paper and the accompanying explanation must be submitted at least 20 working days before its publication.

Notification to Host Member States

Offerors or persons seeking admission must provide the national Member State's authority with a list of intended host Member States and the starting date of the offer/admission. The national authority will notify the host states within five working days.

Communication with ESMA

The national Member State's authority must provide ESMA with the white paper and relevant information, including the starting date of the offer or admission to trading. ESMA will make the white paper available in its register by the start date.

6. Publication of the Crypto-Asset White Paper and Marketing Communications

Publication Requirements

Offerors and persons seeking admission to trading of crypto-assets (other than asset-referenced tokens or e-money tokens) must publish their crypto-asset white papers and marketing communications (if applicable) on a publicly accessible website. The publication must occur reasonably in advance and, at the latest, before the start of the offer to the public or admission to trading. These documents must remain available on the website for as long as the crypto-assets are held by the public.

Consistency with Notified Versions

The published versions of the crypto-asset white paper and marketing communications must be identical to the versions notified to the competent authority [31] or, if applicable, to the modified version [32].

31 As per Article 8 of MiCA

32 In accordance with Article 12 of MiCA

7. Result of the Offer to the Public and Safeguarding Arrangements

Result Publication for Time-Limited Offers

Offerors of crypto-assets with a time limit on the offer must publish the result of the offer on their website within 20 working days of the end of the subscription period.

Ongoing Updates for Non-Time-Limited Offers

Offerors of crypto-assets with no time limit must continuously publish the number of units in circulation at least monthly on their website.

Safeguarding Funds and Crypto-Assets

Offerors of time-limited offers must have effective arrangements to monitor and safeguard the funds or crypto-assets raised. They must ensure these assets are kept in custody by:

- A credit institution (for funds), or
- A crypto-asset service provider offering custody and administration services for crypto-assets.

Safeguarding for Non-Time-Limited Offers

For offers with no time limit, the offeror must maintain the safeguarding arrangements until the retail holder's right of withdrawal[33] expires.

8. Rights of Offerors and Persons Seeking Admission to Trading of Crypto-Assets

Offering and Trading After Publication

Once the crypto-asset white paper (and any modified version) is published[34] offerors may offer crypto-assets throughout the Union. These crypto-assets may also be admitted to trading on a trading platform within the Union.

Exemption from Additional Information Requirements

Offerors and persons seeking admission to trading, having published a white paper, are not subject to further information requirements concerning the public offer or admission to trading of the crypto-asset.

---

33 Under Article 13 of MiCA

34 According to Article 9 of MiCA

9. Modification of Published Crypto-Asset White Papers and Marketing Communications

Requirement for Modification

Offerors, persons seeking admission to trading, or operators of trading platforms for crypto-assets (excluding asset-referenced tokens and e-money tokens) must modify their published crypto-asset white papers and, if applicable, marketing communications whenever there is a significant new factor, material mistake, or inaccuracy that could affect the assessment of the crypto-assets. This requirement applies for the duration of the offer to the public or while the crypto-asset is admitted to trading.

Notification of Modified Documents

The modified crypto-asset white papers or marketing communications, along with the intended publication date and reasons for modification, must be notified to the competent authority of the national Member State at least seven working days before publication.

Public Disclosure of Modifications

On the publication date, or earlier if required by the competent authority, the offeror or operator must notify the public through their website about the modification and provide a summary of the reasons for the changes.

Consistency in Modified Documents

The order of information in modified documents must remain consistent with the original crypto-asset white papers or marketing communications published.

Communication Between Authorities

Within five working days of receiving the modified documents, the competent authority of the national Member State must notify the competent authority of the host Member States and communicate the modification to the European Securities and Markets Authority (ESMA). ESMA will make the modified documents available in its register upon publication.

Publication of Modified Documents

Offerors or platform operators must publish the modified documents, including the reasons for modification, on their websites.

Timestamping and Availability

Modified crypto-asset white papers and marketing communications must be time-stamped, with the latest version clearly marked. All versions must remain publicly available for as long as the crypto-assets are held by the public.

Impact on Utility Token Offers

For utility token offers to provide access to future goods or services, any changes made in the modified documents will not extend the 12-month offer time limit.

Availability of Older Versions

Older versions of the documents must remain publicly available on the website for at least 10 years after publication, with a prominent warning that they are no longer valid and a hyperlink to the most recent version.

10. Right of Withdrawal

Right of Withdrawal for Retail Holders

Retail holders who purchase crypto-assets (excluding asset-referenced tokens and e-money tokens) directly from an offeror or via a crypto-asset service provider may withdraw from the agreement within 14 calendar days without incurring fees or needing to provide reasons. The withdrawal period begins on the date of the agreement.

Reimbursement of Payments

All payments made by the retail holder, including any charges, must be reimbursed without undue delay, no later than 14 days after the offeror or service provider is informed of the withdrawal decision. Reimbursement will be made using the same payment method unless the retail holder agrees otherwise.

Information on the Right of Withdrawal

Offerors must include information on the right of withdrawal in the crypto-asset white paper.

Limitation of the Right of Withdrawal

The right of withdrawal does not apply if the crypto-assets were admitted to

trading before the retail holder purchased them.

Expiration of the Right of Withdrawal

If offerors set a time limit for the public offer of crypto-assets, the right of withdrawal cannot be exercised after the subscription period ends.

11. Obligations of Offerors and Persons Seeking Admission to Trading of Crypto-Assets (Other than Asset-Referenced Tokens or E-Money Tokens)

General Obligations

Offerors and individuals seeking admission to trading of crypto-assets, excluding asset-referenced tokens or e-money tokens, must:

- **Act with Integrity:** They are required to act honestly, fairly, and professionally;
- **Clear Communication:** They must communicate with both holders and prospective holders of the crypto-assets in a fair, clear, and non-misleading manner;
- **Manage Conflicts of Interest:** Identify, prevent, manage, and disclose any conflicts of interest;
- **Maintain Security Standards:** Ensure that all systems and security protocols comply with applicable Union standards. ESMA, in cooperation with EBA, will issue guidelines by 30 December 2024 to specify these standards.

Equal Treatment of Holders

Offerors and individuals seeking admission to trading must act in the best interests of the holders of the crypto-assets, treating them equally unless any preferential treatment is disclosed in the crypto-asset white paper or marketing communications.

Return of Funds in Case of Cancellation

If a public offer for crypto-assets is canceled, offerrs must return any collected funds to holders or prospective holders within 25 calendar days from the date of cancellation.

12. Liability for Information Given in a Crypto-Asset White Paper

Liability for Inaccurate or Misleading Information

Offerors, persons seeking admission to trading, or trading platform operators are liable to holders of crypto-assets for any loss incurred due to incomplete, unfair, or misleading information in the crypto-asset white paper or its modified version. This liability extends to members of their administrative, management, or supervisory bodies.

Exclusion of Contractual Liability

Any contractual exclusion or limitation of civil liability regarding inaccurate or misleading information is legally ineffective.

Responsibility for Information Provided by Trading Platform Operators

When the crypto-asset white paper and marketing communications are prepared by the trading platform operator, persons seeking admission to trading are also responsible for providing accurate, fair, and clear information.

Burden of Proof for Holders

Crypto-asset holders must provide evidence that the offeror, person seeking admission to trading, or platform operator has violated Article 6 of MiCA (see point 3) by providing misleading, incomplete, or unclear information. The holder must also demonstrate that reliance on this information influenced their decision to purchase, sell, or exchange the crypto-asset.

Limitation of Liability Regarding Summaries

Offerors, persons seeking admission to trading, and platform operators are not liable for losses resulting from reliance on information provided in the summary unless:

- The summary is misleading, inaccurate, or inconsistent with the rest of the white paper;
- The summary fails to provide key information needed for prospective holders to make informed decisions.

Preservation of Civil Liability

This point does not affect other civil liability claims that may arise under national law.

VII. Prevention and Prohibition of Market Abuse and Consumer Protection

A. Prevention and prohibition of market abuse involving crypto-assets[35]

1. Scope of the rules on market abuse

Application to Crypto-Assets

This framework applies to actions related to crypto-assets that are either already admitted to trading or for which a request for admission to trading has been submitted.

Coverage of Transactions and Behavior

The rules apply to any transaction, order, or behaviour involving the crypto-assets mentioned above, regardless of whether these actions occur on a trading platform.

Geographical Scope

The framework applies to both actions and omissions concerning crypto-assets, irrespective of whether they occur within the European Union or in third countries.

2. Inside information

Definition of Inside Information

Inside information refers to:

Precise, non-public information concerning one or more issuers, offerors, or persons seeking admission to trading or one or more crypto-assets. The criterion is that if made public, this information would likely impact the prices of the crypto-assets or related crypto-assets.

---

35 The provisions on Market Abuse in the Markets in Crypto-assets (MiCA) Regulation are contained in Title VI, Articles 86 to 92.

- For persons responsible for executing orders for crypto-assets on behalf of clients, inside information also includes non-public information conveyed by clients about pending orders. Again, if made public, this information would likely affect crypto-asset prices or related prices.

Precise Nature of the Information

Information is considered precise if it refers to circumstances that exist or are expected to arise or to events that have occurred or are reasonably expected to occur. It must be specific enough to allow a conclusion about the possible effects on the prices of crypto-assets. In cases of ongoing processes leading to certain events or circumstances, both the final outcome and the intermediate steps may be deemed precise.

Intermediate Steps as Inside Information

An intermediate step in a prolonged process can be regarded as inside information if it meets the above criteria (for example, it must be specific enough to allow a conclusion about the possible effects on crypto-asset prices).

Impact on Prices

Information that, if made public, would likely have a significant effect on crypto-asset prices refers to data that a reasonable crypto-asset holder would likely use in their investment decisions.

3. Public Disclosure of Inside Information

Public Disclosure Requirements

Issuers, offerors, and persons seeking admission to trading are required to publicly disclose inside information (as defined above) that directly concerns them as soon as possible. The disclosure must:

- Enable fast access by the public.
- Ensure complete, correct, and timely assessment of the information.
- Not be combined with marketing activities.

Additionally, issuers, offerors, and persons seeking admission to trading must maintain this disclosed inside information on their websites for a minimum period of five years.

Delaying Disclosure

Issuers, offerors, and persons seeking admission to trading can delay public disclosure of inside information under the following conditions:

- **Legitimate Interests:** Immediate disclosure could harm their legitimate interests.
- **No Misleading Impact:** Delaying the disclosure is unlikely to mislead the public.
- **Confidentiality:** The confidentiality of the inside information can be maintained during the delay.

Informing Competent Authorities

If the disclosure of inside information is delayed, issuers, offerors, or persons seeking admission to trading must:

- Inform the competent authority about the delay and explain how the conditions for delaying the disclosure were met immediately after the information is disclosed to the public.
- Alternatively, Member States may allow a record of the explanation to be provided upon request by the competent authority instead of immediately.

ESMA's Role in Technical Standards

To ensure consistency in the application of this Article, ESMA is tasked with developing draft implementing technical standards for:

- The appropriate means of public disclosure of inside information.
- Procedures for delaying the disclosure of inside information.

ESMA was required to submit these draft standards to the European Commission by 30 June 2024. The European Commission is empowered to adopt these standards as part of the MiCA implementation process.

4. Prohibition of Insider Dealing

Definition of Insider Dealing

Insider dealing occurs when a person who is in possession of inside information:

- Uses that information to acquire or dispose of crypto-assets for their own or a third party's account, directly or indirectly.
- Cancels or amends a crypto-asset order placed before possessing inside information.
- Submits, modifies, or withdraws a bid for their or a third party's account based on inside information.

Prohibition of Insider Dealing

No person can:

- Engage in or attempt insider dealing, either for their own account or for a third party.
- Use inside information to directly or indirectly acquire or dispose of crypto assets.
- Recommend or induce another person to engage in insider dealing.

Recommendations and Inducement

No person in possession of inside information shall:

- Recommend or induce another person to acquire, dispose of, cancel, or amend an order for crypto-assets based on that inside information.

Use of Recommendations

Suppose a person uses a recommendation or inducement based on inside information. In that case, they are engaging in insider dealing if they knew or should have known the recommendation was based on inside information.

Scope of Application

The above rule applies to anyone possessing inside information due to:

- Membership in the administrative, management, or supervisory bodies of the issuer, offeror, or person seeking admission to trading.
- Holding capital in the issuer, offeror, or person seeking admission to trading.
- Accessing information through employment, professional duties, or involvement in distributed ledger technology.
- Involvement in criminal activities.

It also applies to any person who obtains inside information through other means if they know or should have known it is inside information.

Application to Legal Persons

Suppose the insider dealing involves a legal person. In that case, the prohibition applies to the natural persons responsible for the decision to acquire, dispose of, cancel, or amend an order on behalf of the legal person following national law.

5. Prohibition of Unlawful Disclosure of Inside Information

General Prohibition

Individuals possessing inside information are prohibited from unlawfully disclosing such information to others unless it is done in the normal course of their employment, profession, or duties.

Onward Disclosure

Onward disclosure of recommendations or inducements (as referred to in the subtitle Use of Recommendations) constitutes unlawful disclosure if the disclosing party knows or should know that the information was based on inside information.

6. Prohibition of Market Manipulation

General Prohibition

Engaging in or attempting to engage in market manipulation is strictly prohibited.

Definition of Market Manipulation

Market manipulation includes the following activities:

(a) False or Misleading Signals

- Entering transactions, placing orders, or engaging in behaviour that:

1. Gives or is likely to give false or misleading signals about a crypto-asset's supply, demand, or price.
2. Secures or is likely to secure the price of one or more crypto assets at abnormal or artificial levels unless for legitimate reasons.

(b) Deceptive Practices

- Engaging in activities that affect or are likely to affect the price of one or more crypto assets by using fictitious devices, deception, or contrivances.

(c) Dissemination of False Information

- Spreading false or misleading information through the media (including the internet) that:

1. Gives false signals about the supply, demand, or price of crypto-assets.
2. Secures abnormal or artificial price levels of crypto-assets, including disseminating rumors, when the person knows or should have known the information is false or misleading.

Specific Examples of Market Manipulation

(a) Dominant Market Position

- Securing a dominant position over the supply or demand for a crypto-asset, resulting in price fixing or creating unfair trading conditions.

(b) Disruptive Orders

- Placing, modifying, or canceling orders on a trading platform that:

1. Disrupts or delays the platform's normal functioning.
2. Makes it harder for others to identify genuine orders, thereby destabilising the platform.
3. Creates false or misleading signals about the supply, demand, or price of a crypto-asset, particularly by entering orders that exaggerate market trends.

(c) Opinion Manipulation

- Using access to traditional or electronic media to express opinions about a crypto-asset after taking positions on that asset, profiting from the impact on the asset's price without disclosing the conflict of interest to the public clearly and effectively.

Prevention and Detection of Market Abuse

Professional Responsibilities

- Persons professionally involved in arranging or executing transactions in crypto-assets must establish effective systems, arrangements, and procedures to prevent and detect market abuse.
- These professionals are subject to the rules of notification in the Member State where they are registered or have their head office. For branches, the rules apply to the Member State where the branch is located.
- They must report any reasonable suspicion related to orders, transactions (including cancellations or modifications), or aspects of distributed ledger technology, such as the consensus mechanism, which may indicate that market abuse has been or is likely to be committed.

- Reports of suspicious orders or transactions should be sent to the relevant competent authorities, who will then transmit the information to the authorities of the trading platforms concerned.

Regulatory Technical Standards by ESMA

- ESMA is tasked with developing draft regulatory technical standards that further specify the following:
  - Appropriate systems, arrangements, and procedures for compliance with market abuse prevention.
  - The template to be used for reporting suspicious activities.
  - Coordination procedures for detecting and sanctioning market abuse in cross-border situations.
- ESMA is required to submit these draft regulatory technical standards to the European Commission by **30 December 2024**.

Guidelines for Supervisory Practices

To ensure consistency in supervisory practices across Member States, ESMA will issue guidelines by 30 June 2025 on preventing and detecting market abuse. These guidelines will be issued under **Article 16 of Regulation (EU) No 1095/2010** if they are not already addressed by the regulatory technical standards.

B. Consumer protection

The Markets in Crypto-Assets (MiCA) Regulation aims to establish a robust framework for consumer protection within the crypto-asset market, addressing both business-to-consumer (B2C) interactions and the operational standards of crypto-asset service providers. The regulation draws upon existing consumer protection laws and imposes specific obligations on service providers to ensure transparency, integrity, and fairness in their operations.

1. General Consumer Protection Framework

Under MiCA, even though certain crypto-assets are exempt from specific obligations, broader European Union legislative acts, such as Directive 2005/29/EC and Council Directive 93/13/EEC, remain applicable in B2C relationships. These directives ensure that consumer rights are protected when crypto-assets are offered to the public, especially in cases where such assets are marketed or sold.

The continued relevance of these directives guarantees that existing consumer protection measures apply to crypto-asset transactions despite the unique nature of the crypto market[36].

2. Obligations of Crypto-Asset Service Providers

To protect consumers, crypto-asset service providers are required to act with honesty, fairness, and professionalism, prioritising the best interests of their clients. These services, when they meet the criteria set out in Directive 2002/65/EC, are considered "financial services," and the contracts between providers and consumers are subject to the obligations of this directive.

Providers must offer complete, clear, and non-misleading information to clients, including warnings about the inherent risks of crypto-assets. They are also required to make their pricing policies public, establish clear complaints-handling procedures, and develop a strong policy for identifying, preventing, managing, and disclosing conflicts of interest[37].

3. Prudential Requirements

To further safeguard consumer interests, MiCA mandates prudential requirements for crypto-asset service providers. These requirements are set either as a fixed amount or in proportion to the provider's previous year's overheads, depending on the types of services offered. This ensures financial stability and consumer protection by requiring providers to maintain adequate capital reserves to cover potential losses or risks[38].

4. Transparency in Crypto-Asset Exchanges

Crypto-asset service providers that exchange crypto-assets for funds or other crypto-assets using their own capital must adopt non-discriminatory commercial policies. Providers must either publish firm quotes or disclose the methodology for determining asset prices. They are also subject to post-trade transparency requirements to ensure consumers are fully informed about the terms and risks of their transactions[39].

5. Suitability of Crypto-Asset Services and Advice

When providing advice or portfolio management services related to crypto-

36 Point 29 of the preliminary part of MiCA Regulation 2023/1114

37 Point 79 of the preliminary part of MiCA Regulation 2023/1114

38 Point 80 of the preliminary part of MiCA Regulation 2023/1114

39 Point 85 of the preliminary part of MiCA Regulation 2023/1114

assets, providers must assess the suitability of their services or assets for individual clients. This assessment takes into account the client's experience, knowledge, objectives, and ability to bear losses. If a crypto-asset service is deemed unsuitable, providers are prohibited from recommending it or initiating portfolio management. In addition, providers must offer clients detailed reports that include the suitability assessment and periodic updates on the performance of their portfolio[40].

6. Development of Technical Standards

To ensure consistent application of MiCA across the European Union, the regulation entrusts the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) with the development of regulatory technical standards. These standards are essential to maintaining high levels of consumer protection and ensuring that crypto-asset service providers comply with the regulation uniformly[41] .

7. Complaints-Handling Procedures

Issuers of Asset-Referenced Tokens

Issuers of asset-referenced tokens are required to establish transparent and effective complaint-handling procedures for token holders and other interested parties, including consumer associations. This process must be fair, prompt, and consistent, and the procedures must be made publicly available. These complaints-handling obligations also extend to third-party entities involved in the distribution of asset-referenced tokens[42].

8. Competent Authorities

Competent authorities across the Union are responsible for setting up procedures that allow consumers and other stakeholders to file complaints regarding alleged violations of MiCA by issuers, offerors, or service providers. Complaints must be accepted in writing, including electronically, and in the official language of the Member State or another acceptable language[43].

---

40 Point 89 of the preliminary part of MiCA Regulation 2023/1114

41 Point 109 of the preliminary part of MiCA Regulation 2023/1114

42 Article 31 of MiCA Regulation 2023/1114

43 Article 108 of MiCA Regulation 2023/1114

9. Right of Appeal [44]

Member States are required to ensure that decisions made by competent authorities under MiCA are properly reasoned and subject to judicial review. Consumers and other stakeholders, such as public bodies and consumer organisations, are entitled to take legal action before courts or administrative bodies to ensure the proper application of the regulation.

10. Supervisory Measures by EBA

In cases where the issuer of a significant asset-referenced token or e-money token violates the provisions of MiCA, the EBA has the authority to impose corrective measures. These measures include requiring issuers to disclose material information that could impact the market or consumer protection. Such disclosures are critical for ensuring transparency and the smooth operation of the crypto-asset market[45].

44 Article 113 of MiCA Regulation 2023/1114
45 Article 130 of MiCA Regulation 2023/1114

VIII. Powers and cooperation between competent authorities, EBA and ESMA [46]

In accordance with MiCA, 'Competent authority' means one or more authorities:

(a) designated by each Member State concerning offerors, persons seeking admission to trading of crypto-assets other than asset-referenced tokens and e-money tokens, issuers of asset-referenced tokens, or crypto-asset service providers;
(b) designated by each Member State for the application of Directive 2009/110/EC concerning issuers of e-money tokens.

1. Competent Authorities

Designation of Competent Authorities

Member States must designate the authorities responsible for performing the functions and duties outlined in MiCA. These designated authorities must be notified to the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA).

Multiple Competent Authorities

If a Member State designates more than one competent authority, it must clearly allocate specific tasks to each authority. Additionally, the Member State must appoint a single point of contact for cross-border administrative cooperation with other competent authorities and with EBA and ESMA. If necessary, a different single point of contact can be designated for various types of administrative cooperation.

Publication of Competent Authorities

The European Securities and Markets Authority (ESMA) is responsible for publishing a list of the competent authorities designated by Member States on its website.

---

46 The provisions on Powers and cooperation between competent authorities, EBA and ESMA in the Markets in Crypto-assets (MiCA) Regulation are contained in Title VII, Articles 93 to 108.

2. Powers of Competent Authorities

Supervisory and Investigative Powers

Competent authorities are granted the following powers to enforce MiCA:

1. **Information Requests:** Require any person to provide relevant information and documents;
2. **Service Suspension:** Suspend or require suspension of crypto-asset services for up to 30 days if violations are suspected;
3. **Service Prohibition:** Prohibit the provision of crypto-asset services if regulations are infringed;
4. **Disclosure:** Mandate disclosure of material information affecting services, especially to protect retail clients;
5. **Public Disclosure of Non-Compliance:** Publicly announce when a crypto-asset service provider fails to fulfil obligations;
6. **Service Suspension:** Suspend services if providing the service would harm clients, especially retail holders;
7. **Contract Transfer:** Require transfer of contracts to another service provider if authorisation is withdrawn;
8. **Cessation Orders:** Order the immediate cessation of unauthorised activities without prior warning;
9. **White Paper Amendments:** Require amendments to crypto-asset white papers if they fail to meet regulatory requirements;
10. **Marketing Amendments:** Require changes to marketing communications if non-compliant with MiCA;
11. **Additional White Paper Information:** Demand more information in white papers if necessary for market stability or protection of retail holders;
12. **Offer Suspension:** Temporarily suspend offers to the public or admission to trading for up to 30 days if violations are suspected;
13. **Offer Prohibition:** Prohibit offers or admission to trading if regulations are infringed or suspected to be infringed;
14. **Trading Suspension:** Suspend trading on platforms for up to 30 days if violations are suspected;
15. **Trading Prohibition:** Prohibit trading of crypto-assets if regulations are breached or suspected to be breached;
16. **Marketing Suspension/Prohibition:** Suspend or prohibit marketing communications if regulatory violations are suspected;
17. **Suspension of Marketing:** Require cessation of marketing communications for up to 30 days if violations are suspected;
18. **Other Measures:** Take any necessary steps to ensure compliance, including stopping practices or conduct contrary to MiCA;

19. **On-Site Inspections:** Conduct inspections at locations other than private residences to access documents and data;
20. **Outsourced Investigations:** Outsource verifications or investigations to auditors or experts;
21. **Management Removal:** Remove individuals from the management of a service provider or issuer;
22. **Position Reduction:** Require reduction of exposure to crypto-assets;
23. **Online Interface Control:** Order removal or restriction of online interfaces, display warnings, or require hosting service providers to disable access;
24. **Domain Control:** Require domain registries or registrars to delete domain names to allow the authority to register them;
25. **Issuance Restrictions:** Require issuers of asset-referenced tokens or e-money tokens to introduce limits or minimum denominations.

Additional Powers

In addition to the above, competent authorities have these powers:

- Access documents and data and take copies;
- Question individuals involved in operations;
- Seize documents and data if suspected of being relevant to insider dealing or market manipulation;
- Refer cases for criminal prosecution;
- Access existing data traffic records from telecommunications providers if necessary for investigations;
- Request asset freezing or sequestration;
- Impose temporary prohibitions on professional activities;
- Correct false or misleading information and require corrective statements.

Criminal Prosecution

Authorities may refer cases for criminal prosecution.

Court Collaboration

Authorities may also request courts to assist in enforcing powers under national law.

Methods of Exercising Powers

Competent authorities may exercise their powers:

- Directly
- In collaboration with other authorities, including those handling money laundering and terrorist financing;
- Through delegation;
- By application to competent courts.

Member States' Responsibilities

Member States must ensure authorities have appropriate measures to exercise these powers effectively.

Protection for Information Providers

Individuals providing information to authorities under the MiCA are protected from liability for breaching confidentiality obligations.

3. Cooperation Between Competent Authorities

General Cooperation Requirements

Competent authorities must cooperate with each other, as well as the EBA and ESMA, for the purposes of MiCA. They are required to:

- Provide assistance, exchange information without delay, and collaborate on investigation, supervision, and enforcement;
- Ensure that appropriate measures are in place to liaise with judicial and criminal authorities if criminal penalties apply for MiCA infringements.

Grounds for Refusal of Cooperation

Competent authorities can refuse cooperation or information requests in specific cases:

- If the information could impact national security, especially concerning terrorism or serious crimes,
- If cooperation would harm the authority's investigation or enforcement activities;
- If legal proceedings have already been initiated for the same actions;
- If a final judgment has been delivered on the same matter.

Information Exchange

Competent authorities must provide requested information without undue delay to facilitate compliance with the MiCA.

Assistance in On-Site Inspections and Investigations

A competent authority may request help from another Member State's competent authority for on-site inspections or investigations. The requested authority may:

- Conduct the inspection or investigation itself;
- Allow the requesting authority to participate;
- Permit the requesting authority to carry out the inspection or investigation;
- Share specific tasks related to supervision.

ESMA and EBA Coordination

ESMA or EBA may coordinate on-site inspections or investigations when requested by a competent authority, particularly for inspections involving asset-referenced tokens or e-money tokens.

Escalation to ESMA

If a request for cooperation is rejected or delayed, the matter may be escalated to ESMA.

Escalation to EBA

For issues related to asset-referenced tokens or e-money tokens, unresolved requests for cooperation can be escalated to EBA.

Coordinated Supervision

Competent authorities must coordinate their supervision to:

- Identify and address infringement;
- Promote best practices;
- Ensure consistency of interpretation and resolve disagreements;
- Facilitate collaboration across jurisdictions.

EBA and ESMA are responsible for coordinating among authorities and building a common supervisory culture.

Reporting of Infringements

If a competent authority detects non-compliance with the MiCA, it must inform the relevant authority overseeing the entity suspected of the infringement in detail.

Development of Regulatory Technical Standards

ESMA, in cooperation with EBA, developed regulatory technical standards specifying the information to be exchanged between competent authorities. The Commission has the power to adopt these standards.

Development of Implementing Technical Standards

ESMA, with EBA's cooperation, also established standard forms, templates, and procedures for cooperation and information exchange. The Commission was authorised to adopt these standards.

4. Cooperation with EBA and ESMA

Close Cooperation with ESMA and EBA

Competent authorities must collaborate closely with ESMA under Regulation (EU) No 1095/2010 and with EBA under Regulation (EU) No 1093/2010. This cooperation includes the exchange of information necessary for fulfilling their duties under this Regulation.

Provision of Information

Competent authorities are required to promptly provide EBA and ESMA with any information necessary for their respective duties, as per of Regulations above.

Development of Technical Standards

ESMA, in cooperation with EBA, drafted and implemented technical standards that define standard forms, templates, and procedures for cooperation and information exchange between competent authorities, EBA, and ESMA.

5. Promotion of Convergence on the Classification of Crypto-Assets

Joint Guidelines on Crypto-Asset Classification

By December 30, 2024, the European Supervisory Authorities (ESAs) will jointly issue guidelines as per Articles 16 of Regulations (EU) No 1093/2010, No 1094/2010, and No 1095/2010. These guidelines will specify:

- The content and form of the explanation in the crypto-asset white paper;
- Legal opinions on asset-referenced tokens;
- Templates and standardised tests for crypto-asset classification.

Promotion of Consistent Classification Approaches

The ESAs will promote discussions among competent authorities on the classification of crypto-assets. They will identify potential divergences in classification approaches and work toward promoting a unified approach.

Request for Opinion on Crypto-Asset Classification

Competent authorities from home or host Member States may request an opinion from ESMA, EIOPA, or EBA regarding the classification of crypto-assets. The requested authority must provide its opinion within 15 working days, as per the applicable regulatory articles.

Annual Reporting on Classification Difficulties

The ESAs will jointly prepare an annual report based on the information in the register and their activities above. The report will identify challenges in classifying crypto-assets and divergences in the approaches of competent authorities.

6. Cooperation with Other Authorities

Competent authorities must cooperate with other supervisory or oversight bodies responsible for activities not covered by the MiCA. This includes cooperation with tax authorities and relevant supervisory authorities of third countries, as stipulated by Union or national law.

7. Duty of Notification

Obligation to Notify Implementation

Member States are required to notify the Commission, EBA, and ESMA of the

laws, regulations, and administrative provisions implementing this Title, including relevant criminal law provisions, by June 30, 2025.

Notification of Amendments

Member States must promptly inform the Commission, EBA, and ESMA of any subsequent amendments to these laws, regulations, or provisions.

8. Professional Secrecy

Confidentiality of Information

Any information exchanged between competent authorities concerning business, operational, economic, or personal affairs is considered confidential and subject to professional secrecy. Exceptions apply if the information is disclosed for legal proceedings, taxation, or criminal law cases or if the authority permits disclosure.

Obligation of Professional Secrecy

The duty of professional secrecy applies to all individuals or entities who currently work or have worked for the competent authorities. Information subject to professional secrecy cannot be disclosed to third parties unless mandated by Union or national legislation.

9. Data Protection

Compliance with Data Protection Regulations

The processing of personal data by competent authorities under MiCA must comply with Regulation (EU) 2016/679 (General Data Protection Regulation).

Data Processing by EBA and ESMA.

For the purposes of MiCA, personal data processing by EBA and ESMA must be carried out in accordance with Regulation (EU) 2018/1725, which governs data protection within Union institutions and bodies.

10. Precautionary Measures

Notification of Irregularities

When the competent authority of a host Member State suspects irregularities

in the activities of an offeror, a person seeking admission to trading of crypto-assets, the issuer of asset-referenced or e-money tokens, or a crypto-asset service provider, it must notify:

- The competent authority of the home Member State;
- ESMA;
- EBA (if the irregularities involve asset-referenced or e-money tokens).

Measures in Case of Persistent Irregularities

If the irregularities persist despite actions taken by the home Member State's competent authority and they constitute an infringement of MiCA:

- The host Member State's competent authority, after notifying the home Member State, ESMA, and EBA (if relevant), must take appropriate measures to protect crypto-asset clients, particularly retail holders;
- These measures may include preventing the offeror, issuer, or service provider from continuing their activities within the host Member State;
- ESMA and EBA (if applicable) must be informed without delay, and they, in turn, must notify the Commission.

Dispute Resolution

If the home Member State's competent authority disagrees with the measures taken by the host Member State:

- The matter may be referred to ESMA for resolution, applying Article 19(4) of Regulation (EU) No 1095/2010.
- In cases involving asset-referenced or e-money tokens, the issue may be referred to EBA under the provisions of Article 19(4) of Regulation (EU) No 1093/2010.

11. ESMA Temporary Intervention Powers

Temporary Prohibition or Restriction

ESMA may temporarily[47]:

- Prohibit or restrict the marketing, distribution, or sale of certain crypto-assets (excluding asset-referenced tokens or e-money tokens) or of crypto-assets with specific features;

47 In line with Article 9(5) of Regulation (EU) No 1095/2010.

- Prohibit or restrict certain crypto-asset-related activities or practices, excluding asset-referenced tokens or e-money tokens. These measures may apply in specified circumstances or be subject to exceptions.

Conditions for Action

ESMA can take action above only if the following conditions are met:

- **Investor Protection or Systemic Risk:** The action addresses a significant investor protection concern or a threat to market integrity or financial system stability;
- **Inadequate Regulatory Coverage:** Existing Union law regulations do not adequately address the threat;
- **Lack of Competent Authority Action:** Relevant competent authorities have either not taken action, or their actions do not adequately address the issue.

Consideration of Market Impact

When taking action, ESMA must ensure that:

- The measures do not disproportionately harm market efficiency, crypto-asset holders, or service clients relative to the benefits;
- The measures do not lead to regulatory arbitrage.

Notification to Competent Authorities

Before implementing any measures under the first title of this chapter, ESMA must notify the relevant competent authorities.

Public Announcement

ESMA will publish a notice on its website about any decision to impose a prohibition or restriction. The notice will provide details on the measures, which will apply only after the publication date.

Review and Renewal

ESMA must review any prohibition or restriction at least every six months. After two consecutive renewals, ESMA may extend the measure annually, subject to a thorough impact analysis on consumers.

Precedence of ESMA Measures

Any measures taken by ESMA under this chapter will override previous actions taken by relevant competent authorities on the same issue.

Delegated Acts by the Commission

The Commission will adopt delegated acts specifying the criteria and factors for ESMA to determine whether there is a significant investor protection concern, market integrity threat, or systemic financial stability risk.

12. EBA Temporary Intervention Powers

Temporary Prohibition or Restriction

EBA may temporarily:

- Prohibit or restrict the marketing, distribution, or sale of asset-referenced tokens or e-money tokens, or such tokens with specified features;
- Prohibit or restrict specific activities or practices related to asset-referenced tokens or e-money tokens.

These prohibitions or restrictions may apply in specific circumstances or include exceptions as defined by EBA.

Conditions for Action

EBA can take the measures above only if all of the following conditions are met:

- Investor Protection or Systemic Risk: The prohibition or restriction addresses significant investor protection concerns, threats to market integrity, or financial system stability;
- Inadequate Regulatory Coverage: Existing Union laws do not sufficiently address the identified threat;
- Lack of Competent Authority Action: Relevant authorities have either not taken action, or their actions do not adequately address the issue.

Consideration of Market Impact

When taking action, EBA must ensure that:

- The measures do not cause disproportionate harm to market efficiency, token holders, or service clients compared to the benefits;
- The measures do not lead to regulatory arbitrage.

Notification to Competent Authorities

Before taking any measures, EBA must notify the relevant competent authorities of its intended actions.

Public Announcement

EBA will publish a notice on its website detailing any prohibition or restriction imposed. The notice will specify the time from which the measures will take effect, applying only to activities after this point.

Review and Renewal

EBA must review any prohibitions or restrictions at least every six months. After two consecutive renewals, EBA may extend the measures annually, based on a comprehensive consumer impact analysis.

Precedence of EBA Measures

Any measures taken by EBA under this chapter will supersede previous actions taken by competent authorities on the same matter.

Delegated Acts by the Commission

The Commission will adopt delegated acts specifying criteria and factors to be considered by EBA in determining whether there is a significant investor protection concern, market integrity threat, or systemic financial stability risk.

13. Product Intervention by Competent Authorities

Authority to Prohibit or Restrict

A competent authority may prohibit or restrict

- The marketing, distribution, or sale of certain crypto-assets or crypto-assets with specific features;
- Activities or practices related to crypto-assets.

Conditions for Measures

A competent authority may only take action above if it is reasonably satisfied that:

- **Significant Concerns:** The crypto-asset raises substantial investor protection concerns or threatens market integrity or financial stability in at least one Member State;
- **Inadequate Regulatory Coverage:** Existing Union regulations do not sufficiently address these risks, and the issue cannot be better resolved through improved supervision or enforcement of current requirements;
- **Proportionality:** The measure is proportionate, considering the nature of the risks, the sophistication of affected investors, and the likely impact on those holding or using the crypto-asset;
- **Consultation:** The competent authority has consulted other Member States that may be significantly impacted by the proposed measure;
- **Non-discrimination:** The measure does not discriminate against services or activities from other Member States.

The competent authority may impose a precautionary prohibition or restriction even before the crypto-asset has been marketed, distributed, or sold.

Notification Requirements

Before implementing a prohibition or restriction, the competent authority must notify all relevant authorities and ESMA (or EBA for asset-referenced tokens and e-money tokens) at least one month prior to the intended effect. The notification must include:

- The specific crypto-asset or activity subject to the measure;
- Details of the proposed prohibition or restriction and its effective date;
- Evidence supporting the decision and the satisfaction of conditions.

Urgent Measures

In exceptional circumstances, if immediate action is necessary to prevent detrimental effects from a crypto-asset or activity:

- The competent authority may impose an urgent provisional measure with at least 24 hours notice to other competent authorities and ESMA;
- All criteria must still be met, and it must be established that a one-month notice period would be inadequate;

- The duration of provisional measures shall not exceed three months.

Publication of Decisions

The competent authority must publish a notice on its website detailing any prohibition or restriction imposed. This notice shall include:

- Specifics of the prohibition or restriction;
- Effective date post-publication;
- Supporting evidence – the prohibition or restriction will only apply to activities after the measures have taken effect.

Revocation of Measures

A prohibition or restriction must be revoked if the conditions no longer apply.

Delegated Acts by the Commission

The Commission will adopt delegated acts to supplement this regulation by specifying criteria for determining significant investor protection concerns or threats to market integrity or financial stability within at least one Member State.

14. Coordination with ESMA or EBA

Role of ESMA and EBA

Facilitating and Coordinating: ESMA or EBA shall facilitate and coordinate measures taken by competent authorities in accordance with the chapter Product Intervention by Competent Authorities.

Ensuring Justification and Consistency: They are responsible for ensuring that these measures are justified, proportionate, and consistent among competent authorities, where applicable.

Opinion Issuance

Notification and Opinion: Upon receiving notification regarding proposed measures, ESMA or EBA shall issue an opinion on the justification and proportionality of the prohibition or restriction.

Addressing Risks: If ESMA or EBA deems further measures necessary to mitigate risks, it will specify this in its opinion.

Publication: The opinion will be published on the respective websites of ESMA or EBA.

Deviations from Opinions

Notice of Divergence: If a competent authority intends to take measures that differ from or decline to follow the opinion of ESMA or EBA, it must immediately publish a notice on its website, providing a complete explanation of its reasoning.

15. Cooperation with Third Countries

Cooperation Arrangements

Necessity for Agreements: Competent authorities of Member States shall establish cooperation arrangements with supervisory authorities of third countries as needed to facilitate the exchange of information and enforce obligations under the MiCA.

Information Exchange: These arrangements must ensure an efficient exchange of information to enable competent authorities to fulfill their duties.

Notification Requirement: Competent authorities must inform EBA and ESMA, along with other relevant competent authorities, before concluding such arrangements.

Facilitation by ESMA and EBA

ESMA, in collaboration with EBA, shall facilitate and coordinate the development of cooperation arrangements between competent authorities and supervisory authorities of third countries.

Regulatory Technical Standards

To standardise these cooperation arrangements, ESMA and EBA developed regulatory technical standards that provide a template for such agreements.

Information Exchange Coordination

ESMA, in cooperation with EBA, shall facilitate the exchange of information obtained from third-country supervisory authorities that is relevant to the measures.

Professional Secrecy Guarantees

Competent authorities may only exchange information with third-country supervisory authorities if such information is subject to professional secrecy guarantees. This exchange must serve the regulatory tasks of the competent authorities.

16. Complaints Handling by Competent Authorities

Complaint Submission Procedures

Establishment of Procedures: Competent authorities are required to create procedures that allow clients and interested parties, including consumer associations, to submit complaints regarding alleged infringements of MiCA.

Acceptance of Complaints: Complaints can be submitted in writing, including electronically, in an official language of the respective Member State or a language accepted by the competent authorities.

Availability of Information

Communication of Procedures: Information regarding the complaints handling procedures must be accessible on each competent authority's website and communicated to EBA and ESMA.

Publication by ESMA: ESMA shall publish hyperlinks to the relevant sections of competent authorities' websites about complaints handling procedures in its crypto-asset register.

IX. Administrative penalties and other administrative measures by competent authorities, the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA)[48]

1. Administrative Penalties and Other Administrative Measures

Power to Impose Penalties and Measures

Member States must empower competent authorities to impose administrative penalties and measures for specific regulatory infringements, regardless of any criminal penalties or supervisory powers, including violations of:

- Obligations related to white paper information, crypto-asset services, and issuer obligations as set out in specified articles of the MiCA[49];
- Failures to cooperate with investigations or comply with requests for information by competent authorities[50].

If national laws have imposed criminal penalties for any of these infringements by June 30, 2024, Member States can elect not to provide for administrative penalties. Detailed notifications must be sent to the Commission, ESMA, and EBA in such cases.

Minimum Administrative Penalties and Measures for Infringements

Administrative Penalties and Measures for Natural Persons

Member States must ensure that competent authorities have the power to

48 The provisions on Administrative penalties and other administrative measures by competent authorities, EBA and ESMA in the Markets in Crypto-assets (MiCA) Regulation are contained in Title VII, Chapter 3, Article 111 to Article 116.

49 Articles 4 to 14, 16, 17, 19, 22, 23, 25, 27 to 41, 46 to 51, 53 to 55, 59, 60, 64 to 83 and 88 to 92 of MiCA.

50 Article Article 94(3) of MiCA.

impose the following penalties for regulatory infringements:

- **Public Disclosure:** Issuing a public statement identifying the responsible individual or entity and describing the nature of the infringement.
- **Cease-and-Desist Orders:** Requiring the cessation of the infringing conduct and preventing its recurrence.
- **Fines Based on Profits or Losses:** Imposing fines of at least twice the amount of profits gained or losses avoided, regardless of other limits, if such amounts can be determined.
- **Standard Fines:** maximum administrative fines of at least EUR 700 000, or, in the Member States whose official currency is not the euro, the corresponding value in the official currency on 29 June 2023.

Administrative Penalties for Legal Persons

Competent authorities must also be empowered to impose the following fines on legal entities for relevant violations:

- **Fixed Penalties:** The maximum fine is at least EUR 5 million, or, in the Member States whose official currency is not the euro, the corresponding value in the official currency on 29 June 2023
- **Turnover-Based Fines:**
  - **3% of Annual Turnover:** For certain specified compliance violations[51]
  - **5% of Annual Turnover:** For additional specific regulatory breaches[52]
  - **12.5% of Annual Turnover:** For the most serious offences impacting market integrity or operational standards[53].

For entities that are part of a corporate group, fines should be calculated based on the consolidated turnover of the parent company, as outlined in the latest approved financial statements. This ensures the penalties reflect the economic scale of the entire organisation.

In addition to the specified administrative penalties and fines, Member States must ensure that competent authorities have the power to impose a temporary management ban on any member of the management body of a crypto-asset service provider or on any other individual responsible for an

51 3% of turnover for compliance violations under Articles 4-14

53 5% of turnover for infringements under Articles 59, 60, and 64-83

53 12.5% of turnover for repeated or significant violations of Articles 16-41 and 46-47

infringement from performing management roles within a crypto-asset service provider. This measure applies to infringements specified in the regulation in accordance with national law.

Administrative Penalties and Measures for Infringements

Authority of Competent Authorities Member States must ensure that competent authorities have the power to impose a set of administrative penalties and measures for specific regulatory infringements.

Key Penalties and Measures:

1. **Public Disclosure**: A statement identifying the person or entity responsible for the infringement and detailing the nature of the breach.
2. **Cease Orders**: A mandate requiring the responsible party to cease the infringing conduct and refrain from repeating it.
3. **Profit Disgorgement**: Requirement to return any financial gains or avoided losses due to the infringement, where calculable.
4. **Authorisation Suspension or Withdrawal**: Competent authorities may suspend or revoke the authorisation of a crypto-asset service provider.
5. **Management Ban**: A temporary prohibition on individuals responsible for the infringement from holding management roles in crypto-asset service providers. Repeated offences under certain provisions may extend to a ban of at least 10 years.
6. **Trading Ban:** A temporary restriction preventing the individual from engaging in personal trading activities.

Financial Penalties:

- Individuals: Maximum fines of EUR 1 million for specific infringements or EUR 5 million for more severe breaches.
- Legal Entities: Fines up to EUR 2.5 million for certain violations or EUR 15 million (or a percentage of total turnover, if higher).

Additional Powers and Higher Penalties Member States may grant further powers to competent authorities and can set penalty levels exceeding those established here.

2. Determining and Exercising Supervisory and Penalty Powers

Considerations for Imposing Penalties and Measures

When deciding on the type and level of administrative penalties or other

measures, competent authorities must evaluate all relevant factors, including:

1. **Severity and Duration:** The gravity and length of the infringement.
2. **Intent or Negligence:** Whether the act was committed intentionally or negligently.
3. **Degree of Responsibility:** The level of accountability of the individual or entity involved.
4. **Financial Standing:** The financial capability of the responsible party, shown by turnover for legal entities or income and net assets for individuals.
5. **Financial Gains or Avoided Losses:** The amount of profit made or losses avoided by the responsible party, if calculable.
6. **Impact on Third Parties:** Any losses incurred by third parties due to the infringement.
7. **Cooperation with Authorities:** The level of cooperation shown by the infringing party while ensuring any profits gained or losses avoided are recovered.
8. **History of Violations:** Any previous infringements of the Regulation by the responsible party.
9. **Preventive Actions:** Steps taken to prevent future occurrences of the infringement.
10. **Impact on Stakeholders:** The effect of the infringement on crypto-asset holders and clients, especially retail holders.

Coordination and Cooperation in Cross-Border Cases

Competent authorities must work closely to ensure penalties and measures are effective and aligned across jurisdictions. They must coordinate to avoid duplicating efforts or overlaps, particularly in cross-border cases when using their supervisory, investigative, and enforcement powers.

3. Right to Appeal and Consumer Protection Actions

Right of Appeal Against Competent Authority Decisions

- **Appeal Process:** Member States must ensure that all decisions made by competent authorities under this Regulation are well-reasoned and subject to appeal in court.
- **Appeal for Application Decisions:** If no decision is made on an authorisation application with complete information within six months, applicants also have the right to appeal in court.

Consumer Protection Actions by Designated Bodies

- **Eligible Bodies for Legal Action:** To uphold the Regulation, Member States must allow certain entities to take legal action in the interests of consumers:
  - Public Bodies or Representatives: Authorized public entities may initiate court actions.
  - Consumer Organizations: Organizations with a legitimate interest in protecting crypto-asset holders can take action.
  - Professional Organizations: Professional groups may take action on behalf of their members if they have a legitimate interest in compliance with this Regulation.

4. Publication of Decisions on Administrative Penalties and Measures

Timely Publication of Decisions

- The Requirement to Publish: Competent authorities must publish decisions regarding administrative penalties and other measures for regulatory infringements on their official websites without delay after notifying the involved person or entity.
- Content of Publication: The publication should include the infringement's type and nature and the responsible parties' identity. Decisions solely of an investigatory nature are exempt from publication.

Exceptions to Standard Publication

- Disproportionate Impact or Ongoing Investigation: If disclosing identities or personal data is deemed disproportionate or could affect an ongoing investigation, authorities may:
  - Delay Publication: Postpone publication until reasons for withholding cease.
  - Anonymous Publication: Published on an anonymous basis, provided personal data protection remains effective.
  - Non-Publication: Refrain from publishing if anonymity or deferral fails to prevent jeopardising market stability or if the measure is minor.
- Deferred Anonymous Publication: For cases published anonymously, publication may be delayed for a reasonable time until anonymity is no longer necessary.

Appeal Information

Ongoing Appeals: If a penalty or measure is under appeal, authorities must promptly publish this information on their website, including updates on the outcome. Any reversal of a decision must also be published.

Duration of Publication

Five-Year Minimum: Publications must remain accessible on the official website for at least five years, while personal data should be retained only as long as necessary under applicable data protection laws.

5. Reporting of Administrative Penalties and Other Administrative Measures to ESMA and EBA

Annual Reporting Requirements

Aggregate Information Submission
The competent authority is mandated to provide the ESMA and the EBA with annual aggregate data concerning all administrative penalties and measures imposed per Title 1 of this document. ESMA is responsible for publishing this information in its annual report.

Criminal Penalties Reporting
If Member States establish criminal penalties for infringements as outlined in Article 1 of this document, the competent authorities are required to submit anonymised and aggregated data to EBA and ESMA annually. This data should include information on relevant criminal investigations and penalties imposed. ESMA will publish this data in its annual report.

Public Disclosure and Reporting Procedures

Simultaneous Reporting
When the competent authority publicly discloses administrative penalties or criminal penalties, it must simultaneously report these disclosures to ESMA.

Confidential Reporting
Competent authorities are obligated to inform EBA and ESMA about all administrative penalties or measures that have not been published. This includes information about any appeals related to these measures and their outcomes. Furthermore, Member States must ensure that competent authorities obtain information regarding the final judgments of any imposed

criminal penalties and submit this to EBA and ESMA.

Central Database Management

Database Maintenance
ESMA shall maintain a central database containing records of all communicated penalties and administrative measures. This database is intended solely for the exchange of information among competent authorities. Access to this database will be restricted to EBA, ESMA, and competent authorities, and it will be updated based on information provided by these authorities.

6. Reporting of infringements and protection of reporting persons

Directive (EU) 2019/1937 shall apply to the reporting of infringements of this Regulation and the protection of persons reporting such infringements.

X. Supervisory responsibilities of EBA for issuers of significant asset-referenced and e-money tokens and colleges of supervisors[54]

According to MiCA, **'asset-referenced token'** means a type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies.

'Electronic money token' or **'e-money token'** means a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency.

Asset-referenced tokens and e-money tokens **should be deemed significan**t when they meet, or are likely to meet, certain criteria:

- **a large customer base;**
- **a high market capitalisation or**
- **a large number of transactions.**

As such, they could be used by a large number of holders and their use could raise specific challenges in terms of financial stability, monetary policy transmission or monetary sovereignty. Those significant asset-referenced tokens and e-money tokens should, therefore, be subject to more stringent requirements than asset-referenced tokens or e-money tokens that are not deemed significant.

In particular, issuers of significant asset-referenced tokens should be subject to higher capital requirements, to interoperability requirements and they should establish a liquidity management policy. The appropriateness of the thresholds to classify an asset-referenced token or e-money token as significant should be reviewed by the European Commission as part of its review of the application of MiCA. That review should, where appropriate, be accompanied by a legislative proposal.

54 Title VII, Chapter 4, Articles 117 to 120 contain the provisions on EBA's Supervisory responsibilities for issuers of significant asset-referenced and e-money tokens and colleges of supervisors in the Markets in Crypto-assets (MiCA) Regulation.

Risks and Additional Requirements for Significant E-Money Tokens

- **Increased Financial Stability Risks:** Significant e-money tokens (EMTs) pose higher financial stability risks compared to standard e-money tokens and traditional electronic money. Therefore, issuers of significant EMTs must comply with stricter requirements.
- **Higher Capital and Liquidity:** Issuers of significant EMTs, specifically electronic money institutions, are subject to elevated capital requirements, interoperability standards, and must establish a liquidity management policy. They must also follow guidelines similar to those for significant asset-referenced tokens (ARTs) in terms of asset reserve management.
- **Dual Supervision:** Given the extensive usage potential of significant EMTs, dual supervision is necessary. Both the European Banking Authority (EBA) and competent authorities supervise compliance with specific requirements under this regulation. However, credit institutions issuing significant EMTs remain solely under competent authority oversight.

Specific Risks and Supervision of Significant Asset-Referenced Tokens

- **Risks to Monetary Sovereignty:** Significant ARTs can act as a means of exchange for large payment volumes, posing risks to monetary transmission and national monetary sovereignty. The EBA is tasked with supervising significant ART issuers to address these specific risks without setting precedents for other Union legislation.
- **Localised Supervision for Certain Currencies:** If significant EMTs denominated in a non-euro Member State's currency reach high usage within that Member State, EBA supervision may remain with the national competent authority to preserve monetary sovereignty.

1. Supervisory responsibilities of EBA concerning issuers of significant asset-referenced tokens and issuers of significant e-money tokens

Supervisory Scope for Asset-Referenced Tokens

Significant Asset-Referenced Tokens: The European Banking Authority (EBA) overseas issuers of asset-referenced tokens classified as significant according to specified criteria, ensuring compliance through its authority over a set of regulatory powers. These include overseeing issuer operations, reviewing compliance with disclosure requirements, and enforcing measures related to token issuance and market conduct.

Concurrent National Oversight: Where an issuer provides other crypto-asset

services or issues tokens not deemed significant, such services and activities remain under the jurisdiction of the issuer's home Member State authority.

Ongoing Compliance and Reassessment

Compliance Review for Significant Tokens: The EBA is responsible for periodic supervisory reassessments to confirm issuer adherence to the regulatory standards applied to asset-referenced tokens.

Supervisory Scope for E-Money Tokens

Significant E-Money Tokens: For significant e-money tokens issued by licensed electronic money institutions, the EBA supervises issuer compliance with obligations tied to the maintenance of token value and the effective management of customer funds.

Regulatory Enforcement: The EBA exercises additional supervisory powers to uphold these compliance standards, applying specific controls across e-money institution operations related to token issuance, fund safeguarding, and customer interaction.

Collaborative Supervision

Cooperative Framework: The EBA coordinates with other relevant authorities to ensure unified supervision of token issuers, especially with prudential regulatory bodies and competent national authorities within the issuer's operational landscape. This includes, where relevant, collaboration with the European Central Bank (ECB) and supervisory bodies defined under the European Union's banking and financial services regulations.

2. EBA Crypto-Asset Committee

Establishment and Purpose

Formation of the Committee: The European Banking Authority (EBA) will establish a permanent internal crypto-asset committee as mandated by the governance framework of EBA. This committee is tasked with preparing decisions under EBA's oversight functions, specifically those relating to crypto-asset supervision.

Responsibilities of the Committee

Decision Preparation: The committee supports EBA by preparing decisions for

supervisory actions and other responsibilities entrusted to EBA regarding crypto-assets.

Technical Standards: The committee is authorised to draft both regulatory and implementing technical standards, ensuring compliance and consistency in EBA's supervisory functions.

Operational Boundaries

Scope of Activity: The committee is limited to activities outlined for decision preparation, technical standard drafting, and any essential tasks directly related to EBA's crypto-asset responsibilities.

3. Supervisory Colleges for Significant Asset-Referenced Tokens and Significant E-Money Tokens

Establishment and Purpose

Formation of Supervisory Colleges: Within 30 days of classifying an asset-referenced token or e-money token as significant, the European Banking Authority (EBA) must establish, manage, and lead a consultative supervisory college for each significant token issuer. These colleges facilitate coordinated supervision and collaborative activities.

Composition of the Supervisory College

Core Members

The supervisory college includes:

- EBA
- ESMA
- Competent authorities from the home Member State of the issuer
- Authorities overseeing relevant crypto-asset service providers, custodians, and credit institutions
- Authorities of key trading platforms
- Authorities of payment service providers connected to the token
- Authorities of the entities ensuring the functions
- Authorities of the most relevant crypto-asset service providers providing custody and administration of crypto-assets on behalf of clients in relation to the significant asset-referenced tokens or with the significant e-money tokens;
- ECB and central banks where non-euro currencies are involved
- Member States where the token is widely used, upon request
- Relevant supervisory bodies from third countries under agreements with EBA.

EBA may invite other relevant authorities based on the significance of the supervised entities to the college's tasks.

Responsibilities and Coordination

1. **Primary Functions:**
The college
    - Prepares non-binding opinions and facilitates information exchange
    - Agrees on the voluntary distribution of tasks among members
2. **Collaborative Agenda-Setting**
Members can contribute agenda items, promoting inclusivity in college discussions.
3. **Written Agreement on Operations:**
College members must establish a written agreement outlining operational procedures, including voting, meeting frequency, communication protocols, and the potential establishment of multiple colleges for specific asset groups.

Role of EBA as Chair

As chair, EBA:

- Develops operational guidelines, coordinates college activities, and convenes meetings
- Informs members of upcoming meetings, key topics, and decisions made

Standardisation and Technical Standards

Drafting Standards for Consistency

To ensure uniformity across colleges, EBA, in collaboration with ESMA and ECB, will draft standards specifying:

- Criteria for selecting relevant entities (e.g., custodians, trading platforms)
- Conditions for large-scale usage of tokens
- Specific practical arrangements within college operations

Timeline for Draft Standards

EBA will submit these standards to the European Commission by 30 June 2024 for adoption, ensuring alignment with the broader regulatory framework.

4. Non-Binding Opinions of Supervisory Colleges for Significant Asset-Referenced Tokens and Significant E-Money Tokens

Purpose and Scope of Non-Binding Opinions

Areas of Opinion

A supervisory college may issue non-binding opinions on the following key areas:

- Reassessment of issuer supervision as outlined in EBA's supervisory mandate
- Requirements for issuers to hold increased own funds under risk management provisions
- Updates to issuer recovery and redemption plans
- Changes to an issuer's business model
- Modifications to a crypto-asset white paper
- Implementation of corrective measures or supervisory actions
- Administrative agreements with third-country supervisory authorities
- Delegation of supervisory tasks to other competent authorities
- Adjustments to authorisations or oversight measures affecting college members

Inclusion of Recommendations

Upon request and majority approval by the college, opinions may also include recommendations addressing any identified weaknesses in the proposed supervisory measures.

Decision-Making Process within the College

Voting Mechanism

- Each Member State is allocated a single vote within the college, even if represented by multiple authorities.
- The European Central Bank (ECB) has only one vote, regardless of its multiple roles.
- Third-country supervisory authorities in the college do not possess voting rights.

Majority Requirement: College opinions are adopted through a simple majority vote.

Consideration and Response by EBA and Competent Authorities

Response to Non-Binding Opinions: EBA or relevant authorities must carefully consider the college's non-binding opinions, including any recommendations, especially when implementing supervisory measures.

Requirements for Divergent Decisions: If EBA or a competent authority diverges from the college's opinion or recommendations, it must provide a clear rationale explaining the basis for any significant deviations from the college's input.

XI. EBA's powers and competencies for issuers of significant asset-referenced tokens and issuers of significant e-money tokens

The provisions on EBA's powers and competencies for issuers of significant asset-referenced tokens and issuers of significant e-money tokens in the Markets in Crypto-assets (MiCA) Regulation are contained in Title VII, Chapter 5, Article 121 to Article 138.

1. Legal Privilege and EBA's Authority for Information Requests

Protection of Privileged Information

EBA and its authorised officials cannot use their powers to compel disclosure of information covered by legal privilege.

2. Information Requests for Supervisory Responsibilities

Request for Information

To fulfil its supervisory duties, EBA may request necessary information from:

- Issuers of significant asset-referenced tokens or those in control of or controlled by these issuers
- Third parties with contractual arrangements with significant asset-referenced token issuers
- Crypto-asset service providers, credit institutions, or investment firms holding reserve assets
- Issuers of significant e-money tokens and related control entities
- Payment service providers connected to significant e-money tokens
- Distributors of significant e-money tokens on behalf of issuers
- Crypto-asset service providers offering custody and administration of crypto-assets
- Trading platform operators that list significant tokens
- Management bodies of all involved entities

Simple Request for Information

EBA may issue a simple request, which must:

- Reference the legal basis and purpose of the request
- Specify the required information and set a response deadline
- Indicate the request is voluntary but requires truthful responses if complied with
- Inform about potential fines for incorrect or misleading information

Mandatory Information Request by Decision

EBA may issue a formal decision to compel information, including:

- Legal basis, purpose, and specified information
- Deadline for information provision
- Indication of penalties for non-compliance or misleading information
- Notification of rights to appeal within EBA's Board of Appeal and judicial review by the Court of Justice

Obligations of Information Providers

Compliance with Requests: Designated individuals or representatives must provide the requested information, including legally authorised representatives for legal entities.

Notification to Competent Authorities: EBA will promptly inform the competent authority of the Member State where the requested party is located or established about the information request.

3. EBA's General Investigative Powers for Supervision

Investigation Authority and Scope

Authority to Investigate

To fulfil supervisory responsibilities, the EBA can investigate issuers of significant asset-referenced and e-money tokens. Authorised officials may:

- Examine records, data, and other relevant material in any format
- Obtain certified copies or extracts from these materials
- Request oral or written explanations from issuers, management, or staff, and record responses
- Interview other persons who consent to provide relevant information
- Request records of telephone and data traffic

Information Sharing with Supervisory College

Relevant findings from investigations must be promptly communicated to the college for supervisory tasks.

Conducting Investigations

Authorisation Requirements

Authorised officials must present a written authorisation outlining the investigation's subject and purpose, potential penalty payments for non-compliance, and fines for misleading information.

Issuers' Compliance Obligation

Issuers are required to cooperate with EBA investigations. The investigation order specifies:

- Subject and purpose of the investigation
- Details on penalty payments
- Available legal remedies and rights to appeal to the Court of Justice

Coordination with National Authorities

EBA must notify the relevant Member State authority before an investigation. Upon request, local officials can support the investigation and may attend.

Court Authorization for Data Requests

Judicial Authorization

If a request for telephone or data records needs court approval under national law, EBA must apply for this authorisation, which may be sought preemptively.

Court Review of Authorization Requests

When reviewing EBA's request, a court must confirm:

- The authenticity of EBA's decision
- Proportionality of requested measures to prevent excessiveness

EBA Justifications for Proportionality

Courts may request EBA to provide detailed justifications, especially regarding the following:

- Evidence of suspected regulatory violations
- Seriousness and nature of the suspected offence

Courts may not review the necessity of the investigation or demand access to EBA's internal files. Only the Court of Justice can review the lawfulness of EBA's decisions.

4. EBA's Authority for On-Site Inspections

Purpose and Notification of On-Site Inspections

Inspection Purpose

EBA may conduct on-site inspections at the business premises of issuers of significant asset-referenced tokens and significant e-money tokens as part of its supervisory responsibilities. Findings relevant to supervisory tasks must be promptly shared with the supervisory college.

Notification and Coordination

EBA will notify the competent authority of the Member State where the inspection is conducted. However, to maintain the inspection's efficiency, EBA may proceed without prior notice to the issuer, if necessary, after informing the relevant national authority.

Powers and Requirements During Inspection

Authorised Officials' Powers

Authorised EBA officials conducting an on-site inspection may:

- Enter business premises and access all necessary records and data
- Seal business premises, books, or records temporarily if needed for the inspection

Written Authorization

Officials must present a written authorisation detailing the inspection's subject, purpose, and any penalties for non-compliance.

Obligations of Issuers

Issuers of significant asset-referenced or e-money tokens must comply with inspection orders from EBA. The order will specify:

- Subject, purpose, and start date of the inspection
- Penalty payments for non-compliance
- Legal remedies and the right to appeal before the Court of Justice

Support from National Authorities and Court Authorization

Assistance from Member State Authorities

National authorities may be asked to support or attend the inspection, and they must ensure EBA officials receive the necessary assistance. If an issuer opposes the inspection, local authorities may seek police assistance.

Court Authorization

If national law requires judicial authorisation for inspections or assistance requests, EBA will apply for authorisation, which may be sought preemptively.

Court's Role in Reiewing Authorization Requests

The court will ensure:

- Authenticity of EBA's inspection order
- Proportionality of measures taken to avoid excessive or arbitrary actions

For proportionality, the court may request EBA to provide detailed explanations of the suspected regulatory breach and its severity but cannot review the necessity of the investigation or access EBA's internal files. The Court of Justice is the sole body authorised to review the lawfulness of EBA's decision.

5. Exchange of Information

Information Exchange Between EBA and Competent Authorities

Purpose and Scope of Information Sharing

To fulfil supervisory duties, EBA and competent authorities are required to share relevant information promptly. This includes information related to:

- Issuers of significant asset-referenced tokens and controlling entities
- Third parties with contractual arrangements with significant asset-referenced token issuers
- Crypto-asset service providers, credit institutions, or investment firms holding reserve assets
- Issuers of significant e-money tokens and controlling entities
- Payment service providers associated with significant e-money tokens
- Entities distributing significant e-money tokens on behalf of issuers
- Crypto-asset service providers managing assets for clients involving significant tokens
- Trading platforms listing significant asset-referenced or e-money tokens
- Management bodies of the entities mentioned above

Conditions for Refusal of Information Exchange

Grounds for Refusal

Competent authorities may refuse information exchange or cooperation in investigations or on-site inspections only under the following conditions:

- Compliance would adversely affect ongoing investigations or criminal proceedings
- Judicial proceedings for the same actions have already commenced in the Member State
- A final judgment for the same actions has already been issued within the Member State

6. Administrative agreements on the exchange of information between EBA and third countries

Conditions for Agreements

EBA may establish administrative agreements with supervisory authorities in third countries for information exchange, provided that:

- The disclosed information is protected by professional secrecy standards equivalent to EBA's.

Purpose of Information Exchange
The exchanged information should serve the supervisory responsibilities of EBA or the corresponding third-country supervisory authorities.

Personal Data Transfers
EBA must comply with EU Regulation 2018/1725 when transferring personal data to third countries.

7. Disclosure of Information from Third Countries

Conditions for Disclosure
EBA may disclose information received from third-country supervisory authorities only if:

- Explicit consent is obtained from the third-country authority that provided the information or
- Disclosure is essential for judicial proceedings.

Exceptions to Agreement Requirement
The requirement for explicit agreement does not apply when information is requested by:

- Other Union supervisory authorities for fulfilling their tasks
- Courts for investigations or proceedings related to criminal penalties

8. Cooperation with Other Authorities

Collaborative Oversight
For issuers engaged in activities outside the scope of this regulation, EBA will coordinate with other relevant supervisory authorities, including:

- Tax authorities
- Supervisory bodies of third countries not involved in the supervisory college

9. Professional secrecy

The obligation of professional secrecy shall apply to EBA and all persons who work or who have worked for EBA as well as to any other person to whom EBA has delegated tasks, including auditors and experts contracted by EBA.

10. Supervisory Measures by the EBA

A. Measures Concerning Significant Asset-Referenced Tokens

Infringements and Actions

1. **Issuance of Cease Orders**
   - The EBA may require the issuer to cease any conduct constituting an infringement.
2. **Imposition of Penalties**
   - The EBA may impose fines or periodic penalty payments as outlined in chapters 15 and 16 of this document.
3. **Request for Additional Information**
   - Issuers may be required to provide supplementary information to protect holders, especially retail holders.
4. **Suspension of Offers**
   - Offers to the public may be suspended for a maximum of 30 consecutive working days if there are reasonable grounds for suspicion of regulatory infringement.
5. **Prohibition of Offers**
   - The EBA may prohibit public offers if infringements are confirmed or suspected.
6. **Trading Suspension**
   - Crypto-asset service providers may be required to suspend token trading for up to 30 consecutive working days on reasonable suspicion of infringement.
7. **Trading Prohibition**
   - Trading may be prohibited on platforms if an infringement is confirmed.
8. **Amendment of Marketing Communications**
   - Issuers may be instructed to amend marketing communications.
9. **Suspension or Prohibition of Marketing Communications**
   - Marketing communications may be suspended or prohibited if regulatory breaches are suspected.
10. **Disclosure of Material Information**
    - Issuers must disclose all material information affecting the assessment of the asset-referenced token to ensure consumer protection and market operation.
11. **Issuance of Warnings**
    - The EBA may issue warnings regarding non-compliance with obligations.
12. **Withdrawal of Authorization**
    - Authorisation of the issuer may be withdrawn.

13. **Removal of Management**
    - The EBA may require the removal of individuals from the issuer's management body.
14. **Minimum Denomination or Issuance Limit**
    - Issuers may be required to introduce a minimum denomination or limit the amount issued.

B. Measures Concerning Significant E-Money Tokens

Infringements and Actions

1. **Issuance of Cease Orders**
    - Similar to asset-referenced tokens, issuers must cease any conduct constituting an infringement.
2. **Imposition of Penalties**
    - Fines or periodic penalty payments may also be applied as per chapters 15 and 16 of this document.
3. **Request for Additional Information**
    - Issuers may be required to provide supplementary information for the protection of holders, particularly retail holders.
4. **Suspension of Offers**
    - Offers to the public may be suspended for up to 30 consecutive working days on reasonable suspicion of infringement.
5. **Prohibition of Offers**
    - Offers may be prohibited if infringements are confirmed or suspected.
6. **Trading Suspension**
    - Trading of significant e-money tokens may be suspended for a maximum of 30 consecutive working days under similar conditions.
7. **Trading Prohibition**
    - Trading may be prohibited on platforms where infringements are confirmed.
8. **Disclosure of Material Information**
    - Issuers must disclose material information that impacts the assessment of the significant e-money token.
9. **Issuance of Warnings**
    - Warnings regarding non-compliance may be issued.
10. **Minimum Denomination or Issuance Limit**
    - Issuers may be required to introduce a minimum denomination or limit the amount issued.

C. Considerations for Measures

The EBA will consider the following when taking measures:

- **Duration and Frequency:** Length and recurrence of the infringement.
- **Financial Crime:** Whether the infringement facilitated financial crime.
- **Systemic Weaknesses:** There are serious weaknesses in issuer procedures or risk management.
- **Intentionality:** Whether the infringement was committed intentionally or negligently.
- **Responsibility Degree:** Level of issuer responsibility for the infringement.
- **Financial Strength:** The issuer's financial capability is based on turnover or assets.
- **Impact on Holders:** Effect on interests of holders of the tokens.
- **Profit Impact:** Importance of profits gained or losses avoided by the issuer.
- **Cooperation Level:** Degree of cooperation with the EBA during investigations.
- **Previous Infringements:** History of prior infringements by the issuer.
- **Preventative Measures:** Actions taken post-infringement to prevent recurrence.

D. Notification and Disclosure Procedures

Notification to ESMA and Central Banks: Before measures related to points d. to g. and j. from point a) are taken, the EBA must inform ESMA, the ECB, or relevant central banks as necessary.

Issuer Notification: The EBA must promptly notify the issuer responsible for the infringement and relevant competent authorities of any measures taken.
Public Disclosure: The EBA must publicly disclose decisions on its website within 10 working days unless such disclosure jeopardises financial stability or causes disproportionate harm. Disclosures will not include personal data.

Public Statements

Public disclosures must affirm the following:

- The right to appeal decisions.
- Any relevant appeals lodged that do not have suspensive effects.

The possibility for EBA's Board of Appeal to suspend contested decisions per Article 60(3) of Regulation (EU) No 1093/2010.

---

11. Fines Imposed by the EBA

Conditions for Imposing Fines

Grounds for Decision

The EBA shall impose a fine if it determines that:

- An issuer of a significant asset-referenced token or a member of its management body has committed an infringement as listed in Annex V, either intentionally or negligently.
- An issuer of a significant e-money token or a member of its management body has committed an infringement as listed in Annex VI, either intentionally or negligently.

Intentional Infringement: An infringement is deemed intentional if the EBA finds objective factors indicating deliberate action by the issuer or management member.

Considerations for Fines

When determining the fine, the EBA shall consider the following factors:

1. **Nature and Seriousness:**
   - Duration and frequency of the infringement.
   - Occurrence or facilitation of financial crime attributable to the infringement.
2. **Systemic Weaknesses:**
   - Existence of serious or systemic weaknesses in the issuer's procedures, policies, or risk management measures.
3. **Intent vs. Negligence:**
   - Whether the infringement was committed intentionally or negligently.
4. **Responsibility Degree:**
   - The degree of responsibility of the issuer for the infringement.
5. **Financial Strength:**
   - The financial capability of the issuer is based on total turnover or annual income and net assets.
6. **Impact on Holders:**
   - Effect of the infringement on the interests of holders of significant asset-referenced or e-money tokens.
7. **Profit and Loss Considerations**:
   - Importance of profits gained or losses avoided by the issuer due to the infringement.

8. **Cooperation Level:**
   - The issuer's cooperation with the EBA while ensuring disgorgement of profits gained or losses avoided.
9. **Previous Infringements:**
   - History of prior infringements by the issuer.
10. **Preventative Measures:**
   - Actions taken by the issuer after the infringement to prevent recurrence.

Maximum Fine Amounts

For Issuers of Significant Asset-Referenced Tokens
The maximum fine shall be:

- Up to **12.5%** of the annual turnover for the preceding business year or
- Twice the amount of profits gained or losses avoided due to the infringement, if determinable.

For Issuers of Significant E-Money Tokens
The maximum fine shall be:

- Up to **10%** of the annual turnover for the preceding business year, or
- Twice the amount of profits gained or losses avoided due to the infringement, if determinable.

12. Periodic Penalty Payments

Purpose of Periodic Penalty Payments

Objectives

The EBA shall impose periodic penalty payments to ensure compliance with the following:

- **Cease Infringing Conduct**: To compel a person to stop conduct constituting an infringement as outlined in previous supervisory measures.
- **Information Provision**: To require individuals referenced in the applicable regulations to:
  - Provide complete information requested by EBA.
  - Submit to an investigation, including the production of complete records, data, and other required materials.
  - Comply with an on-site inspection as ordered by EBA.

Conditions for Imposing Penalties

(A) Characteristics

Effectiveness and Proportionality:

- The periodic penalty payment must be effective and proportionate to the infringement.
- The payment shall be imposed for each day of delay in compliance.

(B) Calculation of Amounts

Amount Specification:

- The periodic penalty payment shall amount to the following:
  - **3%** of the average daily turnover for the preceding business year for legal entities.
  - **2%** of the average daily income for the preceding calendar year for natural persons.
- This calculation starts from the date specified in the EBA's decision imposing the penalty.

Duration of Periodic Penalty Payments

Imposition Period

- Periodic penalty payments shall be enforced for a maximum period of **six months** following the notification of EBA's decision.
- At the end of this period, the EBA shall review the necessity and effectiveness of the measure.

13. Disclosure and Enforcement of Fines and Periodic Penalty Payments
Public Disclosure of Fines and Penalties

Disclosure Requirements
The EBA shall publicly disclose every fine and periodic penalty payment imposed in accordance with the specified regulations, except in cases where such disclosure:

- Would seriously jeopardize financial stability.
- Would cause disproportionate damage to the involved parties.

Personal Data Protection: The disclosed information shall not include any personal data.

Nature and Enforceability of Fines

Fines and periodic penalty payments imposed are categorized as administrative measures.
The enforcement of fines and periodic penalty payments shall adhere to the civil procedure rules in effect within the jurisdiction where the enforcement takes place.

Allocation of Funds

The amounts collected from fines and periodic penalty payments shall be allocated to the general budget of the Union.

Non-Imposition of Fines or Penalties

In cases where the EBA opts not to impose fines or penalty payments despite the previous regulations, it shall:

- Notify the European Parliament, the Council, the Commission, and the competent authorities of the relevant Member State.
- Provide an explanation outlining the reasons for its decision.

14. Procedural rules for taking supervisory measures and imposing fines

Appointment and Role of Investigation Officer

Appointment Criteria

- The EBA shall appoint an **independent investigation officer** if there are clear grounds to suspect an infringement.
- The officer must be independent and uninvolved in prior supervision of the concerned issuers.

Responsibilities and Independence

- The officer conducts the investigation independently, collecting evidence and examining any comments from the investigated parties.
- After investigation, the officer submits a file of findings to the EBA.

Powers and Access of the Investigation Officer

Investigation Powers: The officer may request information as per regulatory provisions and conduct investigations and on-site inspections in accordance with regulatory guidelines.

Access to Information: The officer has access to all relevant documents gathered by the EBA during supervision.

Rights of the Investigated Parties

Opportunity to Respond

- Before finalizing the report, the officer must allow the investigated parties to comment on the findings.
- Findings are based solely on facts for which the parties have had an opportunity to respond.

Right to Defense: The defense rights of the concerned parties shall be fully respected throughout the investigation.

Access to File: Investigated parties have access to the investigation file, except for confidential third-party information and EBA's internal documents.

EBA Decision-Making Process

Determining Infringements

- Based on the investigation file, and after hearing from the investigated parties if requested, the EBA decides if an infringement occurred.
- If an infringement is found, EBA shall:
  - Implement **supervisory measures** in line with regulatory standards.
  - Impose fines as outlined in the applicable provisions.

Non-Participation of Investigation Officer: The investigation officer is excluded from EBA's decision-making process.

Delegated Acts by the Commission

Regulatory Requirements: The commission adopted delegated acts to clarify procedural rules for fines and penalty payments and provisions on defence rights, fine collection, and limitation periods.

Referral to National Authorities

Referral for Criminal Investigation: If the EBA finds indications of potential criminal offences, it shall inform the national authorities for further investigation and possible prosecution.

Non-Duplication of Penalties: The EBA shall not impose fines if a final acquittal or conviction for the same facts has been reached in national criminal proceedings (res judicata).

15. Hearing of Persons Concerned in Supervisory Decisions

Right to Be Heard

- Prior to finalising any supervisory or penalty decision, EBA provides individuals or entities under investigation the opportunity to respond to its findings.
- EBA will base its decisions exclusively on findings that the investigated parties have had the chance to review and comment on.

Exception for Urgent Action

- In cases requiring immediate action to avert significant or imminent threats to financial stability or to crypto-asset holders (especially retail holders), EBA may enact an interim decision without prior consultation.
- In such instances, EBA will ensure that the concerned parties have an opportunity to be heard as promptly as possible following the interim decision.

Rights of Defense and File Access

- EBA respects the defence rights of those under investigation, ensuring access to the investigative file.
- Access limitations apply to confidential information, business secrets of other parties, and EBA's internal preparatory documents to protect sensitive material.

16. Review by the Court of Justice

The Court of Justice holds extensive authority to review EBA's administrative decisions that impose fines, periodic penalties, or other measures.

The Court may:

- Annul the decision;
- Reduce the imposed penalty;
- Increase the fine or penalty if deemed appropriate.

17. Imposition of Supervisory Fees

Obligation to Pay Fees

- EBA imposes fees on issuers of significant asset-referenced tokens and significant e-money tokens.

- These fees cover EBA's supervision costs, as well as any expenses incurred by competent authorities, engaged in oversight under delegated tasks.

Calculation of Fees

- Fee for Asset-Referenced Token Issuers
  - Proportional to the size of reserve assets.
  - Covers all supervisory expenses incurred by EBA under this regulation.
- Fee for E-Money Token Issuers
  - Based on the size of issuance in exchange for funds.
  - Encompasses all costs for EBA's supervisory activities, including reimbursements to competent authorities.

Delegated Act by the European Commission

The Commission issued a delegated act detailing:

- Types of fees;
- Matters for which fees are due;
- Calculation method and payment process;
- Maximum fee per entity.

18. Delegation of tasks by EBA to competent authorities

Delegation Framework

EBA may delegate specific supervisory tasks to competent authorities as needed for effective oversight of issuers of significant asset-referenced or e-money tokens.

Delegated tasks can include powers to:

- Request information under specified guidelines;
- Conduct investigations and on-site inspections.

Consultation Requirements

Prior to delegating any task, EBA must consult with the relevant authority to determine:

- Scope and extent of the task;
- Timetable for task completion;
- Required information-sharing protocols.

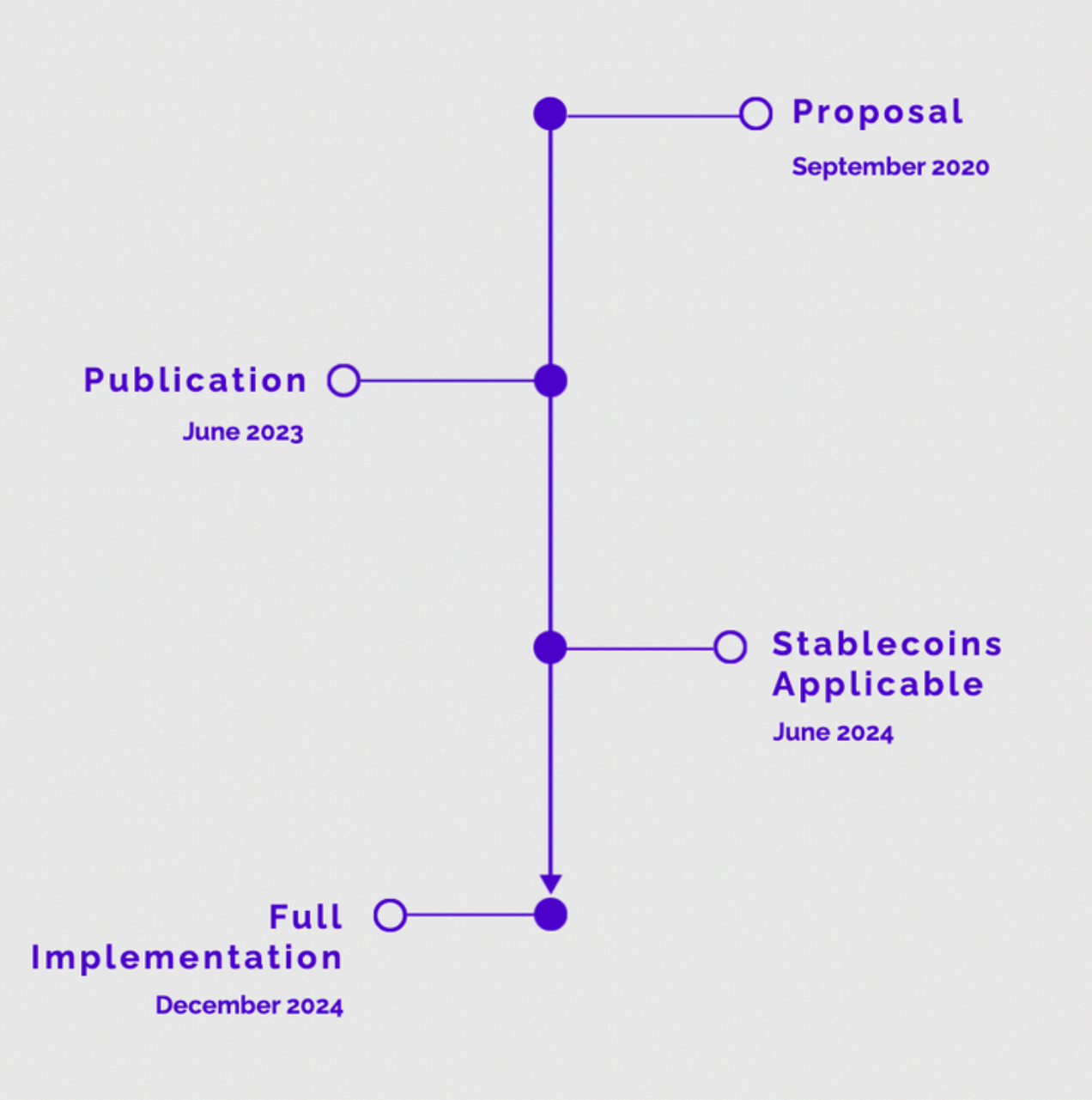
Cost Reimbursement

Reimbursement Protocol: EBA will reimburse competent authorities for costs incurred in delegated tasks, as per the fee delegation framework specified by the Commission.

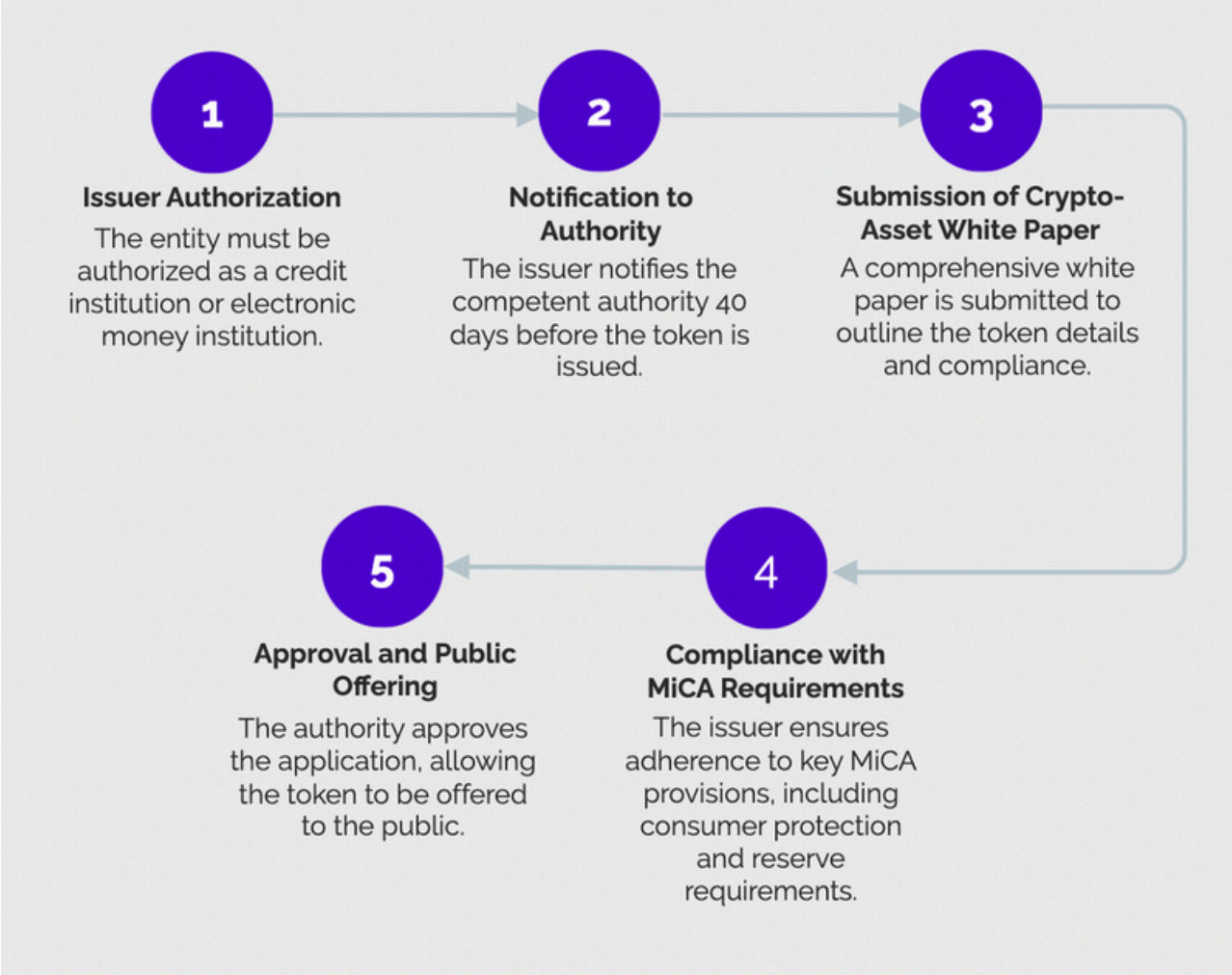
Review and Revocation

Ongoing Oversight: EBA will periodically review delegated tasks to ensure effectiveness and may revoke delegation as necessary.

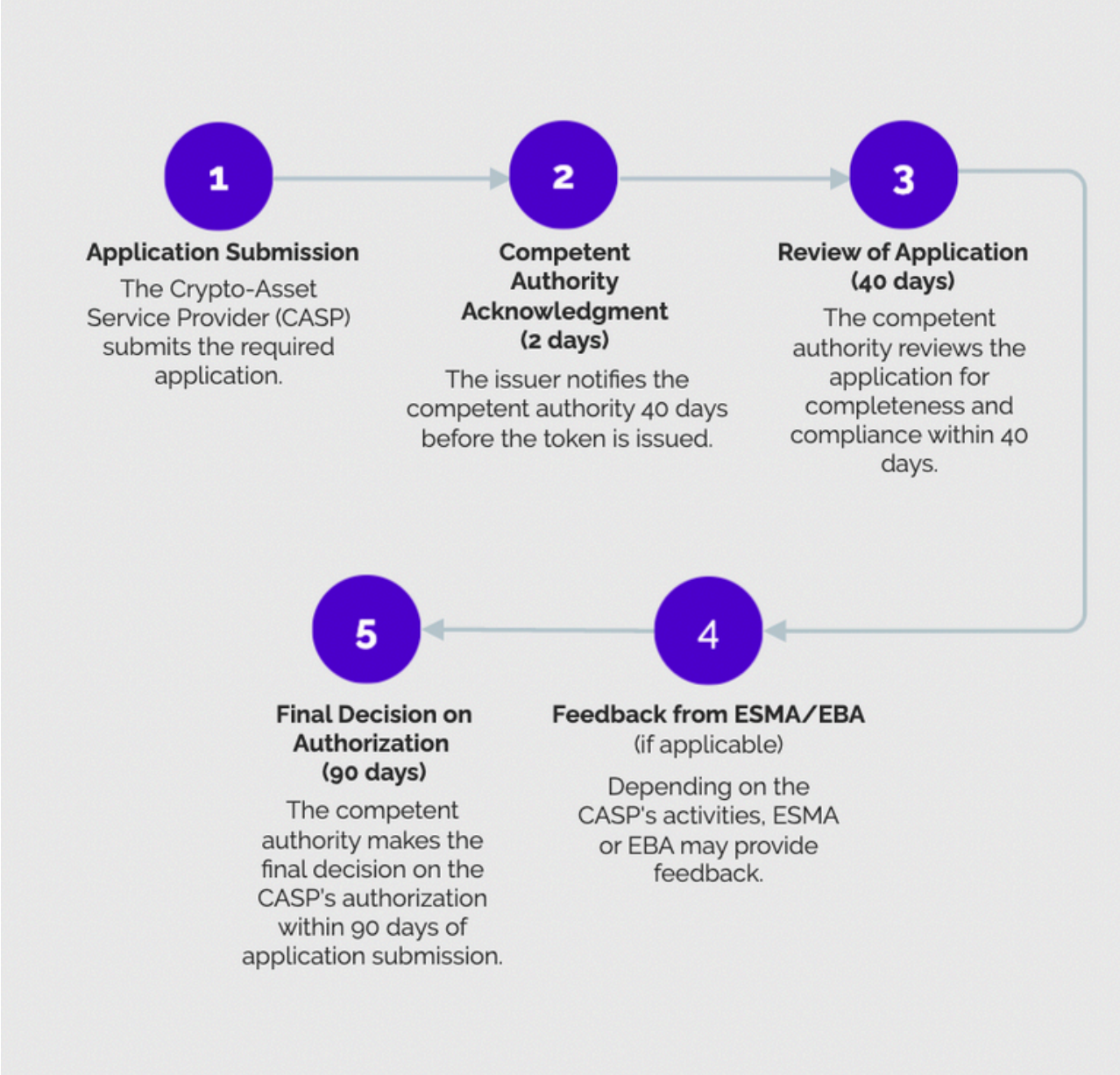
MiCA Implementation Timeline



The E-Money Token (EMT) Licensing Process



CASP Licensing Process under MiCA



Maximum fines under MiCA