

European Commission

**Directorate-General for Financial Stability,
Financial Services and Capital Markets Union**

SPA 2 – Pavillon Rue de Spa 2 / Spastraat 2
Bruxelles / Brussel
Belgique / België

E-Mail: fisma-mica-review@ec.europa.eu

Ref. No. FMA-LE0001.230/0005-INT/2026
(To be quoted in further correspondence!)

Department Integrated Supervision &
Innovation

Expert

Jakob Deutsch

Phone +43 1 249 59-4217

E-Mail jakob.deutsch@fma.gv.at

Vienna, 29.09.2026

**Austrian FMA's contribution to the European Commission's targeted consultation on
the review of Regulation on the Markets in Crypto-Assets**

Dear Sir or Madam,

Having regard to the European Commission's targeted consultation on the review of Regulation on the Markets in Crypto-Assets we would like to provide you with the attached official contribution of the Austrian Financial Market Authority (FMA).

The contribution has also been submitted via the ECAS EU Survey Tool using the link on the page https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-review-mica-regulation_en for easier processing.

We kindly ask you to take our contribution into consideration.

Financial Market Authority
On behalf of the Executive Board

Christoph Seggermann

Fabian Aubrunner

signed electronically

	Unterzeichner	Österreichische Finanzmarktaufsichtsbehörde
	Datum/Zeit-UTC	2026-09-30T12:40:42+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.fma.gv.at/amtssignatur
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	

Targeted consultation on the review of Regulation on the Markets in Crypto-Assets (MiCA)

Introduction

Background for this consultation

[Regulation 2023/1114 of 31 May 2023 on Markets in Crypto-Assets \(MiCA\)](#), which sets a dedicated and harmonised framework at Union level to provide specific rules for crypto-assets and related services and activities started to apply in part from 30 June 2024 and in full from 30 December 2024.

Crypto-assets and distributed ledger technology (DLT) offer opportunities for faster cross-border payments, new fundraising methods, and innovative decentralised services, but also entail risks. MiCA was introduced to provide legal certainty through a harmonised EU framework, defining key crypto-asset categories and setting requirements for issuers and service providers, while fostering responsible innovation and mitigating risks related to investor protection, market integrity, and financial stability. As these markets are growing in importance, and traditional financial services providers are also moving into the crypto- and tokenised assets space, a question arises whether the regulatory framework currently governing them remains fit for purpose. The national competent authorities (NCAs), the [ESA](#) and the industry have been sharing feedback on their first implementation experiences. While it may be difficult at this stage to draw conclusions on how MiCA is performing in practice, there have been many policy and regulatory developments globally since MiCA was adopted, and more importantly the crypto-asset markets themselves have significantly developed and continue to evolve since MiCA was designed and adopted. Given these developments, the Commission services consider it necessary to compare and contrast, via this public consultation, the EU framework for crypto-assets with the more recent frameworks of other jurisdictions and with market developments. The results should help assess whether MiCA remains fit for purpose in this evolving policy and market context. Notwithstanding the objective to promote innovation and digitalisation in European financial systems, financial regulation should remain technology neutral. This is crucial to guarantee the freedom of choice for market participants without inciting them towards using any specific technology and to ensure financial regulation remains adapted to technological advancements without major amendments.

Article 142 MiCA requests the Commission to present a report to the European Parliament and the Council on the latest developments with respect to crypto-assets, in particular, on matters that were left outside the scope of MiCA. The Commission services consider that the review of the Payment Services Directive has largely addressed and clarified some issues emerging from the interplay between the payment services legislation and MiCA following the [advice of the EBA](#). This consultation, the Commission services therefore:

- seek to respond to the request in Article 142 of MiCA¹ and seek to collect the views of the stakeholders on all the market developments not originally covered by MiCA and whether policy or regulatory action would be warranted (see part 5)
- seek feedback to inform the review of MiCA referred to in Article 140 of MiCA², consulting also the [EBA](#) and the [ESMA](#) to that effect
- seek to consult on matters that have emerged from the implementation of MiCA to date
- take stock of whether MiCA is fit for the future in the rapidly evolving landscape of digital and tokenised asset markets in a global and internationally competitive context, seizing both the opportunities tokenisation and DLT bring and addressing risks they may generate

In line with its simplification agenda to support EU competitiveness, the Commission services also wish to

¹ Regulation (EU) 2023/1114, Article 142(1): 'By 30 December 2024 and after consulting EBA and ESMA, the Commission shall present a report to the European Parliament and the Council on the latest developments with respect to crypto-assets, in particular on matters that are not addressed in this Regulation, accompanied, where appropriate, by a legislative proposal'.

² Regulation (EU) 2023/1114, Article 140(1): 'By 30 June 2027, having consulted EBA and ESMA, the Commission shall present a report to the European Parliament and the Council on the application of this Regulation accompanied, where appropriate, by a legislative proposal. An interim report shall be presented by 30 June 2025, accompanied, where appropriate, by a legislative proposal'.

use this consultation to gather information and assess whether administrative or other burdens emanating from MiCA and its implementation measures can be simplified, reduced or dispensed with.

Beyond questions related to crypto-assets covered by MiCA, this consultation puts forward several questions affecting broader financial acquis. Interested parties that wish to bring other relevant issues, not raised in this consultation, to the Commission's attention, should feel free to communicate them through the open question at the end of this questionnaire. The Commission services welcome specificity and brevity in the replies. The different parts of the consultation cover the following areas:

- **PART 1 - Scope and definitions (title II crypto-assets):** this section includes questions on the current conditions for offering or seeking admission to trading of crypto-assets other than asset referenced tokens (ARTs) or e-money tokens (EMTs)
- **PART 2 - requirements applying to asset referenced tokens (ARTs) and e-money tokens (EMTs) and their issuers (titles III and IV):** this section includes questions on the current conditions for offering or seeking admission to trading of ARTs and EMTs, their prudential regime, the multi-issuance model of global tokens and considering also the interaction with third country regulatory frameworks, the reserve requirements of ARTs and EMTs, the redemption rights of their holders and crisis management measures
- **PART 3 - the appropriateness of the current legal framework for crypto-asset service providers (CASPs) (titles V and VI):** this section covers questions on the adequacy of the current scope of crypto-asset services regulated under MiCA. Since the supervisory arrangements for CASPs are covered under the current [market integration and supervision package \(MISP\)](#), supervision of CASPs is outside the scope of this consultation
- **PART 4 - topics beyond the initial scope of MiCA:** this final part of the consultation consists of questions relating to decentralised finance, crypto-assets staking, lending and borrowing activities, and non-fungible tokens (NFTs). It also seeks views on whether MiCA should aim to increase legal certainty of crypto-assets and other on-chain assets, particularly in relation to natively issued assets

Responding to this consultation

In this targeted consultation, the Commission is interested in the views of a wide range of stakeholders. Responses to this consultation are expected to be most useful where they present a clear and detailed narrative, demonstrated by data (where possible), concrete examples, legal references and qualitative evidence. Specific suggestions for solutions to address issues raised are welcome.

All interested stakeholders are invited to reply by 31 August 2026 via the online questionnaires below.

To the extent that not all questions will be relevant to all stakeholders, respondents are invited to reply only to those questions that are relevant to them.

PART 1: Scope and definitions, Title II crypto-assets

MiCA covers three types of crypto-assets: asset-referenced tokens (ARTs), electronic money tokens (EMTs) and crypto-assets other than ARTs or EMTs. The provisions related to the last category are set out in Title II of MiCA. This part of the consultation seeks feedback on the regulation of this category of crypto-assets.

Crypto-assets that fall under other sectoral legislation such as deposits, financial instruments including derivatives, or other regulated products, are outside the scope of MiCA. Therefore, some crypto-assets are regulated under MiCA, while tokenised financial instruments are not.

The distinction between crypto-assets regulated under MiCA and those governed by other sectoral legislation can sometimes be complex, particularly given that the definitions of certain assets, such as securities, are established in national law. Evolving market practices further highlight the convergence between the two areas, as traditional financial institutions increasingly offer MiCA-regulated crypto-assets and services, while MiCA-authorised entities expand into traditional financial products, subject to obtaining the necessary authorisations to do so.

1.1. MiCA scope & crypto-asset classification

Question 1. Should crypto-assets that qualify as financial instruments defined in [Directive 2014/65/EU](#) of the European Parliament and of the Council, continue to be governed by sectoral legislation ([MiFID/MiFIR/MAR/Prospectus Regulation](#), etc.), or should all assets that are recorded and transacted on distributed ledgers and that meet the definition of a crypto-asset, or the services provided on such assets, in principle be covered by MiCA?

- ☒ Yes, they should remain under the main sectoral legislation
- ☐ No, all crypto-assets, or the services provided on such assets, should be covered by MiCA
- ☐ Don't know / no opinion / not applicable

Question 1.1. Is the distinction between financial instruments governed by MiFID and crypto-assets governed by MiCA sufficiently clear, also taking into account ESMA's guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments?

- ☐ Yes, sufficiently clear
- ☒ No, clarification is needed
- ☐ Don't know / no opinion / not applicable

Please explain and motivate your answers to question 1 and 1.1:

From an FMA perspective, the current boundary is conceptually correct: if an instrument qualifies as a financial instrument under MiFID II, the applicable securities and market rules should continue to apply irrespective of the technology used for issuance, recording or transfer. Tokenisation must not become a route to regulatory downgrade. If all DLT-recorded assets were moved into MiCA-appliance solely because of their technological form, traditional instruments such as shares, bonds or fund interests could be structured on-chain to avoid stricter disclosure, conduct, market abuse and prospectus requirements.

MiFID II / MiFIR, MAR and the Prospectus Regulation provide a more developed and more robust investor-protection and market-integrity framework than Title II MiCA. This is particularly relevant for disclosure quality, ongoing obligations, conflict management, market abuse controls and supervisory intervention. The principle should therefore remain that the same economic function and same risk profile should lead to the same regulatory treatment. Technology should not determine the legal regime. At the same time, practical uncertainty remains in borderline cases, especially where token features are mixed, rights are drafted in novel ways, or national interpretations of “transferable securities” and other financial instruments diverge. Clarification is therefore still needed at EU level as well as a better definition of ARTs, to prevent ARTs from being classified as financial instruments in most if not all cases. Thus, further clarification is needed – especially regarding the distinction between financial instruments governed by MiFID II and ARTs governed by MiCAR. Under the current legislation even a prototypical ART will in most if not all cases be classified as a financial instrument under MiFID II.

Question 1.2: Please explain your answer to question 1.1 and suggest any policy actions for clarification if needed:

see above Q 1

Please explain and motivate your answer to question 1:

see above Q 1

The distribution or storage via a digital ledger is merely one of several characteristics of the product and not decisive for the regulation of the product. Far more important aspects are relating to valuation, liquidity, disclosure requirements, redemption rights, the legal status of token holders, and similar issues (e.g., co-ownership rights versus contractual claims), depositary obligations as well as matters of liability and criminal responsibility. The MiCAR regime is not suitable for addressing these aspects. Consequently, it is absolutely necessary that these instruments remain under the sectoral legislation.

Question 2. To what extent have ESMA’s MiCA Article 2(5) guidelines and the joint ESA standardised classification test reduced uncertainty in practice? Which borderline cases remain difficult?

Please explain your response and suggest any policy actions for clarification if needed.

The Guidelines have reduced uncertainty to a meaningful extent but have not eliminated it. The remaining uncertainty is concentrated in borderline and hybrid cases:

- hybrid tokens combining use/access functions with profit rights, redemption claims or governance rights;
- governance tokens that in practice create an economic expectation similar to equity or fund participation;
- synthetic exposure tokens and perpetual / derivative-like token structures;
- assets marketed as NFTs but issued in series or with de facto fungible features.

Suggested policy action: Develop further common EU case studies, maintain a supervisory repository of anonymised classification outcomes, issue additional guidance and consider a structured escalation mechanism for difficult cases to avoid divergent NCA practice.

1.2. Transparency rules and ex post supervisory control regime

Question 3. Title II establishes disclosure, marketing, conduct and liability rules for public offers and admission to trading of crypto-assets other than ART and EMT.

How appropriate or effective is the design of Title II in balancing investor protection, market integrity and innovation?

a) Please assess each provision below along their adequacy:

	1 (completely inadequate)	2 (mostly inadequate)	3 (neutral)	4 (moderately inadequate)	5 (fully adequate)	Don't know - No opinion - Not applicable
Exemptions for offers to <150 persons per Member State, small offerings (< € 1m over 12 months), and qualified investors (Article 4(2))	☐	☐	☐	☐	☒	☐
White paper disclosure framework (Article 6): issuer information, crypto-asset characteristics, tokenomics, risks, use of proceeds	☐	☐	☐	☒	☐	☐
Marketing requirements: identifiable, fair, clear, not misleading and consistent with the white paper (Article 7)	☐	☐	☐	☐	☒	☐
Ex ante notification model without prior regulatory approval (Article 8)	☐	☒	☐	☐	☐	☐
Obligation to modify/update the white paper for significant new factors, material mistakes or inaccuracies (Article 12)	☐	☐	☐	☐	☐	☒
Retail investor right of withdrawal (14 days), excluding assets already admitted to trading or after subscription period ends (Article 13)	☐	☐	☐	☐	☒	☐
Conduct obligations: honesty, fairness and professionalism, clear communications, conflicts management, and effective systems and security	☐	☒	☐	☐	☐	☐

arrangements (Article 14)						
Civil liability for inaccurate, misleading or incomplete white paper information (Article 15)	☐	☐	☐	☐	☒	☐
Overall balance between investor protection, market integrity and innovation under Title II	☐	☐	☐	☒	☐	☐

Please explain your ratings in question 3 a), focusing on the issues you deem most significant regarding the overall balance between investor protection, market integrity and innovation:

(4) Ex ante notification model: The quality of scrutiny and therefore the whitepapers seem to vary widely between member states which leads to regulatory arbitrage and differing expectations of issuers.

(7) Conduct obligations: From our view the current provision has no material impact on issuers or supervision.

b) Please assess each provision below along the direction of change you consider appropriate:

	1 (should be significantly weakened)	2 (should be somewhat weakened)	3 (should remain unchanged)	4 (should be somewhat strengthened)	5 (should be significantly strength-ened)	Don't know - No opinion - Not applicable
Exemptions for offers to <150 persons per Member State, small offerings (<€ 1m over 12 months), and qualified investors (Article 4(2))	☐	☐	☒	☐	☐	☐
White paper disclosure framework (Article 6): issuer information, crypto-asset characteristics, tokenomics, risks, use of proceeds	☐	☐	☐	☒	☐	☐
Marketing requirements: identifiable, fair, clear, not misleading and consistent with the white paper (Article 7)	☐	☐	☒	☐	☐	☐

Ex ante notification model without prior regulatory approval (Article 8)	☐	☐	☐	☒	☐	☐
Obligation to modify/update the white paper for significant new factors, material mistakes or inaccuracies (Article 12)	☐	☐	☐	☐	☐	☒
Retail investor right of withdrawal (14 days), excluding assets already admitted to trading or after subscription period ends (Article 13)	☐	☐	☒	☐	☐	☐
Conduct obligations: honesty, fairness and professionalism, clear communications, conflicts management, and effective systems and security arrangements (Article 14)	☐	☐	☐	☒	☐	☐
Civil liability for inaccurate, misleading or incomplete white paper information (Article 15)	☐	☐	☒	☐	☐	☐
Overall balance between investor protection, market integrity and innovation under Title II	☐	☐	☐	☒	☐	☐

Please explain your ratings in question 3 b), focusing on the issues you deem most significant regarding the overall balance between investor protection, market integrity and innovation:

(2) White paper disclosure framework: While the information is mostly adequate it could be strengthened with regard to information on the financial background and the specific operations / business model of the issuer. Currently, much energy is focused on the crypto-asset itself as well as underlying technology while the most relevant factor in the future development of the project in our views relies on the financial resilience of the issuer. If the issuer slides into insolvency it will usually be the end of the project.

(4) Ex-ante notification: If the ex-ante notification model without prior approval is to be continued, there is a strong need on additional guidance and provisions to ensure harmonization between Member States.

(9) Overall balance: Investor protection could be further strengthened by increasing the disclosed information regarding financial stability and a more detailed description of liabilities, cooperation partners and business model of the issuer.

Question 4. Based on initial implementation experience under MiCA, please assess the extent to which the following issues remain a concern:

	1 (not serious concern at all)	2 (rather not serious concern)	3 (neutral)	4 (rather serious concern)	5 (extremely serious concern)	Don't know - No opinion - Not applicable
Inadequate or non-comparable disclosure clarity or complexity to retail investors in Title II white papers	☐	☐	☐	☒	☐	☐
Fraudulent or misleading crypto-asset offerings affecting EU investors	☐	☐	☐	☐	☒	☐
Lack of clear and enforceable investor rights for crypto-asset holders	☐	☐	☐	☒	☐	☐
Insufficient issuer governance or accountability in crypto-asset projects e.g. monitoring of the use of funds by issuers after the offering period	☐	☐	☒	☐	☐	☐
Regulatory arbitrage, including activity shifting outside the EU	☐	☐	☐	☐	☒	☐
Promotions by social media, influencers, sponsorships	☐	☒	☐	☐	☐	☐
Post-issuance token value erosion or project failure affecting EU retail investors	☐	☐	☐	☒	☐	☐
Market manipulation practices (e.g. wash trading, price manipulation) in crypto-asset markets	☐	☐	☐	☐	☐	☐
Misaligned incentives Between crypto-asset issuers and investors (e.g. insider allocations, weak lock-ups)	☐	☐	☐	☐	☐	☒

Difficulty in assessing issuer quality and project credibility for EU investors	☐	☐	☐	☐	☒	☐
Cross-border enforcement and supervisory coordination challenges within the EU	☐	☐	☐	☐	☒	☐
Cross-border enforcement and supervisory coordination challenges with third countries authorities outside of the EU	☐	☐	☐	☐	☒	☐

Please explain your ratings in question 4, focusing on the issues you deem most significant and add any additional issues that you deem highly important:

- (1) Some of the information included in white papers seems quite technical while other, more relevant information (financials) is barely mentioned.
- (2)/(3) In some cases token have no use case; it is simply circular financing without any returns in the future. The fact that those products are notified with a NCA gives them more credibility and increases the risk of misleading investors.
- (5) Supervisory approaches to white paper scrutiny differ significantly across Member States. Activity shifting outside of the EU is also a threat, especially regarding the extensive use of “reverse solicitation” methods.
- (7) As many of the envisaged projects probably will not reach their primary goals, there is a significant risk that retail investors finance projects without any return.
- (10) As there is little to none disclosure obligations addressing these issues, they remain a serious concern.

Allocation of Competent Authorities in Cross-Border Market Abuse Cases:

MiCAR lacks clear rules for allocating cross-border market abuse cases between competent authorities. This may lead to overlapping investigations, enforcement gaps, legal uncertainty and risks related to the *ne bis in idem* principle. The Commission should therefore consider introducing objective case-allocation criteria at Level 1.

Title VI of MiCAR (Art 86-92) establishes a comprehensive market abuse framework for crypto-assets, including provisions on inside information, insider dealing, unlawful disclosure, market manipulation and the obligation to report suspected market abuse. However, MiCAR does not contain a jurisdictional anchor for market abuse cases or criteria for determining which competent authority should assume primary responsibility in cross-border investigations.

This omission is particularly significant given the inherently cross-border nature of crypto-asset markets. Issuers, CASPs, trading venues, investors and

affected markets are frequently located in different Member States, while the relevant conduct may have effects across the Union simultaneously. MiCAR does not establish a mechanism for allocating jurisdiction where several authorities may have a legitimate supervisory interest.

Article 95 MiCAR requires competent authorities to cooperate and exchange information but does not determine which authority should act as lead supervisor in a cross-border market abuse case. Likewise, the RTS under Article 92 improve coordination and information-sharing but do not resolve the underlying question of supervisory responsibility.

The absence of a clear lead-authority model may result in duplicative investigations, inconsistent supervisory outcomes and increased compliance burdens. Consideration should therefore be given to introducing a dedicated framework establishing objective criteria for determining the competent lead authority, allocating primary responsibility for investigations and enforcement actions and providing mechanisms for resolving jurisdictional disputes.

A future level 1 framework could build on practical supervisory approaches that use the relevant trading platform as the primary jurisdictional anchor. As a general rule, competence should lie with the authority responsible for the relevant trading platform, which typically has access to the necessary trading and surveillance data and is best placed to assess the conduct concerned. This would also be consistent with Article 92 MiCAR, pursuant to which STORs are transmitted to the competent authority of the relevant trading platform.

Where conduct affects multiple trading platforms, in principle, competence could be assigned to the authority of the most relevant trading platform. This would require objective criteria, for example based on trading activity or trading volumes, as well as a reliable data basis comparable to FIRDS data under MAR.

Allocation of Competent Authorities with regard to issuer-obligations

The NCA of the Member State in which the issuer has its registered office should be responsible for supervising and enforcing issuer-related obligations (Art 88 and 91(2)(c) MiCAR), as it is closest to the issuer and can obtain relevant information most efficiently. This should apply irrespective of where the crypto-asset whitepaper was notified or on which trading platforms the crypto-assets are listed.

For third-country issuers, competence should rest with the authority of the Member State in which the most relevant trading platform for that issuer is located. The place of whitepaper notification and listing venues should be irrelevant for determining competence.

More generally, MiCAR itself should clearly determine which authority is competent in a given case, with deviations permitted only in exceptional circumstances, such as where the designated authority is unable to investigate or sanction violations. This would enhance legal certainty and reduce coordination burdens that may otherwise delay supervisory and enforcement proceedings.

Question 5. Should additional measures either at the issuance stage or during the marketing and distribution of crypto-assets, be considered? Based on your experience or expertise, please evaluate the potential effectiveness of the following additional measures in relation to Title II crypto-assets.

	1 (not at all effective)	2 (slightly effective)	3 (moderately effective)	4 (rather serious concern)	5 (extremely serious concern)	Don't know - No opinion - Not applicable
Marketing restrictions for high-risk or speculative crypto-assets aimed at retail investors e.g. restricting or banning the use of algorithmic or "gamified" marketing tactics for new token launches	☐	☐	☐	☒	☐	☐
Lock-up periods (e.g. 12 months) or vesting schedules for founder and early investor tokens	☐	☐	☐	☒	☐	☐

Please explain your ratings in question 5, and what (other) regulatory or supervisory actions you would consider useful either at the issuance stage and during marketing or distribution:

From a consumer protection perspective, both measures strengthen investor protection. Marketing restrictions reduce the risk of uninformed decisions by retail investors. Lock-up periods and vesting arrangements mitigate the risk of short-term token sell-offs. Both measures should be supported by appropriate transparency requirements.

- Mandatory disclosure of insider allocations, vesting terms, treasury wallet concentration and related party arrangements.
- Clear rules for marketing through affiliates, influencers and sponsorships, including accountability of the issuer / offeror.
- Enhanced requirements for high-risk offerings, including more financial information regarding the respective companies / company groups.

Question 6. What administrative simplification or burden reduction measures should be considered under title II and its implementing measures and technical standards?

Introduce a harmonised EU notification package and mandatory common templates for Title II whitepapers and update notifications.

Create a functioning ESMA-Register to provide a proper overview of the market.

Clarify, through further guidance, what constitutes a "significant new factor", "material mistake" or "inaccuracy" in the MiCAR-setting under Article 12, in order to reduce defensive over-reporting and divergent supervisory practice.

Question 7. Which specific categories remain most difficult to classify in practice? (e.g. hybrid tokens, wrapped assets, tokenised fund interests, tokenised money-market instruments, governance tokens, synthetic exposures, or assets marketed as NFTs but issued in series)?

Hybrid tokens combining utility, governance and economic / profit-related features.

Governance tokens that are marketed as functional but create an investment expectation through fee rights, treasury exposure or de facto control rights.

Synthetic exposure tokens and derivative-like structures.

Assets presented as NFTs but issued in series or with materially fungible economic characteristics.

The most difficult cases are those where legal qualification requires a deeper analysis of the total arrangement: contractual rights, governance design, economic function, marketing, redemption features and the relationship between on-chain and off-chain claims. Especially when token resemble other products (transferable securities, alternative investment funds, utility token vs. ART) the classification often remains uncertain.

Question 8. Are the current Title II mechanisms sufficient to ensure meaningful updates to investors after issuance, including where project governance, tokenomics, vesting schedules or control rights change materially?

☐ Yes

☒ No

☐ Don't know / no opinion / not applicable

Please explain your answer to question 8:

The obligation to provide post-issuance updates applies only for the time of the public offering / duration of the listing. There are no post-issuance updates whatsoever after the offering (which could only last for a few days) is finished. For a total overhaul of the current function or business model after the end of the offering there are no mandatory reporting or updates for issuers.

PART 2. Requirements applying to Assets referenced tokens (ART) and electronic money tokens (EMT) and their issuers (MiCA Titles III and IV)

MiCA establishes a bespoke regulatory regime for so-called “stablecoins” by distinguishing between asset-referenced tokens (ARTs) and e-money tokens (EMTs).

This section seeks stakeholders’ feedback on stablecoins (EMTs and ARTs) in general, notably on the future role they may play both within the EU and beyond. It also asks more specific questions related to their prudential regime, their reserve requirements, the redemption rights of their holders and whether MiCA’s stablecoin regime remains fit for purpose or requires adjustment in view of market and international regulatory developments.

2.1. The future role of stablecoins

Question 9. Looking 5-10 years ahead, how strongly do you agree with the following visions for the role of stablecoins in the EU?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
A mainstream digital means of payment for retail transactions within the EU	☐	☒	☐	☐	☐	☐
A mainstream digital means of payment for wholesale transactions within the EU	☐	☐	☒	☐	☐	☐
A complement to existing payment instruments, used mainly in specific use cases especially in international, cross-border payments	☐	☐	☒	☐	☐	☐
A core infrastructure layer for the digital economy and tokenised financial markets especially for settlement	☐	☐	☐	☒	☐	☐
A niche or transitional product, eventually displaced by other forms of digital money (e.g. CBDCs or commercial bank money innovations)	☐	☐	☐	☒	☐	☐
No clear long-term role can be identified at this stage	☐	☐	☒	☐	☐	☐
Others	☐	☐	☒	☐	☐	☐

Please specify to what other vision(s) you refer in your answer to question 9:

Please explain your answer to question 9:

The FMA considers that the long-term role of stablecoins in the EU remains uncertain.

With regard to retail payments, current evidence does not suggest that stablecoins are likely to become a mainstream means of payment within the EU.

The European payment market is already well served by efficient and widely adopted electronic payment solutions, including card payments, instant payments and account-based payment services. Available market observations indicate that payment-related use cases represent only a limited share of stablecoin activity compared to trading and investment-related uses.

Regarding wholesale payments and settlement, the future role of stablecoins is equally uncertain. The Eurosystem is actively exploring solutions to enable DLT-based settlement using central bank money, including initiatives such as Pontes and Appia. To the extent that DLT-based financial markets can be supported by central bank settlement infrastructures, the incentive to rely on privately issued stablecoins may be reduced.

Cross-border payments are frequently cited as a key use case for stablecoins. However, the realization of this vision would require globally accepted infrastructures (multi chain solutions) combining low transaction costs, scalability, legal certainty and trusted intermediaries (like credit institution or payment providers). While stablecoins may offer benefits in jurisdictions characterized by weak domestic currencies, high inflation or limited access to banking services, these conditions are generally not present in advanced economies such as the EU and the United States. Moreover, there is currently limited evidence of strong demand among users in developed markets to move away from established payment and settlement arrangements.

For tokenised financial markets, similar questions arise. If central bank money becomes available for DLT-based settlement, either directly or through interoperability solutions, it is not evident that privately issued stablecoins will become the preferred settlement asset for wholesale transactions.

Overall, the FMA considers that stablecoins are likely to remain a niche product or a complementary payment and settlement instrument rather than developing into a dominant form of digital money. The future evolution of stablecoins will depend significantly on developments in central bank money infrastructure, tokenised financial markets and payment system interoperability.

More fundamentally, questions remain regarding the long-term sustainability of stablecoin business models. Market activity continues to be concentrated in a limited number of issuers and use cases, and it remains uncertain whether stablecoins can achieve durable adoption outside the crypto-asset ecosystem when competing with regulated payment infrastructures, commercial bank money and potential future central bank digital money solutions.

Question 10. The following question explores the current and potential benefits of stablecoins (both EMTs and ARTs) for different use cases. For each use case below, please indicate how beneficial stablecoins would be for EU users:

	1	2	3	4	5	Don't know - No opinion - Not applicable
	(not beneficial)	(moderately beneficial)	(neutral)	(beneficial)	(very beneficial)	

International payments (non-EU cross-border remittances or transfers)	☐	☐	☐	☒	☐	☐
Intra-EU payments (domestic and EU cross-border payments)	☐	☒	☐	☐	☐	☐
Crypto trading and liquidity provision	☐	☐	☐	☐	☒	☐
Retail payments - Person to Person	☐	☒	☐	☐	☐	☐
Retail payments – Person to Business (POI payment to merchants including e-commerce)	☐	☒	☐	☐	☐	☐
Retail payments - Business to Business	☐	☒	☐	☐	☐	☐
Wholesale payments (between financial institutions)	☐	☐	☒	☐	☐	☐
Settlement of tokenised financial instruments (e.g., digital bonds, securities)	☐	☐	☒	☐	☐	☐
Corporate treasury management	☐	☐	☒	☐	☐	☐
Access to programmable or smart contract-based financial services (DeFi applications)	☐	☐	☒	☐	☐	☐
Provision of financial services in underserved regions in the EU	☐	☐	☐	☒	☐	☐
Others	☐	☐	☐	☐	☐	☐

Please explain shortly your assessment and expectations in question 10 as regards the benefits of stablecoins for EU users and, where relevant, any potential risks:

Please specify to what other use case(s) you refer in your answer to question 10:

See answer Q 9.

2.2. Prudential regime and capital requirements

MiCA sets out different capital requirements for issuers of EMTs and ARTs, with additional requirements applying where tokens are classified as “significant”. Article 35 and 46 require that non-bank issuers of ARTs and EMTs shall, at all times, have own funds equal to an amount of at least the highest of the following:

- a. EUR 350 000
- b. 2% of the average amount of the reserve of assets referred to in Article 36
- c. a quarter of the fixed overheads of the preceding year

Question 11.1. To what extent do you think the calculation methods are relevant?

	1 (not relevant)	2 (slightly relevant)	3 (moderately relevant)	4 (mostly relevant)	5 (highly relevant)	Don't know - No opinion - Not applicable
Minimum own funds of EUR 350,000	☐	☐	☐	☐	☒	☐
2% of the average reserve of assets	☐	☐	☐	☐	☒	☐
25% of the fixed overheads of the preceding year	☐	☐	☐	☐	☒	☐
Additional own funds for “significant” tokens	☐	☐	☐	☐	☒	☐

Question 11.2 To what extent do you think the calculation methods are appropriately calibrated?

	1 (not relevant)	2 (slightly relevant)	3 (moderately relevant)	4 (mostly relevant)	5 (highly relevant)	Don't know - No opinion - Not applicable
Minimum own funds of EUR 350,000	☐	☐	☐	☐	☒	☐
2% of the average reserve of assets	☐	☐	☐	☐	☒	☐
25% of the fixed overheads of the preceding year	☐	☐	☐	☐	☒	☐
Additional own funds for “significant” tokens	☐	☐	☐	☐	☒	☐

Please explain your answers to question 11.1 and 11.2, including your reasoning and any suggestions for recalibration or alternative approaches (e.g. greater risk sensitivity, differentiation by business model, or interaction with reserve and liquidity requirements):

The FMA broadly agrees that the current calculation methods are relevant and appropriately calibrated based on the experience gained so far with the

MiCA framework.

Given the limited implementation experience to date, particularly in light of the absence of authorised ART issuers and the still developing EMT market, the FMA does not currently see a compelling need for more complex or risk-sensitive calculation methodologies. The existing framework combines fixed minimum own funds requirements, reserve-based requirements, fixed overhead requirements and additional requirements for significant tokens, thereby providing a balanced and proportionate prudential framework.

The FMA therefore considers the current methodology to be sufficiently robust for the present stage of market development and would favour maintaining the existing approach until further supervisory experience has been acquired.

While the interaction between MiCA own funds requirements and those applicable to other regulated activities may warrant further clarification, the FMA does not currently consider the introduction of additional risk-based calculation methods or significantly broader supervisory discretion to be necessary. Such changes could increase complexity, reduce legal certainty and potentially undermine the harmonised nature of the framework before sufficient evidence has emerged that the existing regime is inadequate.

The FMA therefore supports continued monitoring of the effectiveness of the current framework and reassessment once more practical experience has been gained with a broader range of issuers, business models and market conditions.

Question 12. After being in effect for close to two years, no ARTs have been licensed in the EU under MiCA. In your view, does this absence primarily reflect low market interest in ARTs or other reasons?

Please rate each factor below:

	1 (not at all a factor)	2 (rather not a factor)	3 (neutral/uncertain)	4 (rather a factor)	5 (a major factor)	Don't know - No opinion - Not applicable
Market interests for ARTs	☐	☐	☐	☒	☐	☐
Licencing and regulatory requirements for ARTs	☐	☐	☐	☐	☒	☐

Please explain your answers to question 12:

The FMA does not consider the absence of authorised ARTs to be primarily the result of a lack of market interest. In practice, a number of market participants have explored ART structures, particularly commodity-linked tokens, including gold-linked arrangements.

The FMA considers licensing and regulatory requirements to be a significant factor explaining the limited number of authorised ARTs. In particular, issuers face substantial challenges in structuring an ART in a manner that clearly falls within the MiCA framework while avoiding classification under existing financial services legislation.

The boundaries between ARTs, financial instruments and alternative investment funds are often difficult to determine in practice. This is compounded by

the fact that certain key concepts used in these frameworks are not fully harmonised at EU level. As a result, considerable legal and structuring uncertainty exists during the product development phase.

The challenges are particularly evident in relation to commodity-linked tokens. In order to comply with MiCA requirements, issuers may need to implement reserve arrangements that ensure a high level of asset protection and insolvency remoteness. Depending on the legal structure used under national civil law, such arrangements may themselves create characteristics that resemble collective investment undertakings or alternative investment funds, potentially leading to a different regulatory classification than initially intended.

This creates a situation where issuers seeking to structure an ART may face considerable legal costs and uncertainty in ensuring that the product simultaneously complies with MiCA while avoiding unintended classification as a financial instrument or an investment fund.

In addition, the FMA notes that the commercial viability of ART issuance may be challenging in some cases given restrictions affecting the monetisation of reserve assets and other prudential requirements. This may further reduce incentives for firms to pursue authorisation despite existing market interest.

The FMA therefore considers that the European Commission should assess whether the current regulatory framework provides a sufficiently clear and operational distinction between ARTs, financial instruments and investment funds. More explicit Level 1 clarification of these boundaries would reduce legal uncertainty and facilitate consistent supervisory outcomes.

More fundamentally, the European Commission should consider whether it intends ARTs to play a meaningful role within the EU crypto-asset ecosystem. If so, greater legal certainty regarding the relationship between MiCA, securities law and investment fund legislation may be necessary to enable the practical development of ART structures within the Union.

Question 13. If ARTs were to come to market, what do you think is the primary purpose from a consumer/investor perspective: investment or alternative means of exchange/payment? Please explain your answer:

The FMA considers that, if ARTs were to emerge at scale, their primary use case would likely be investment and value storage rather than use as a means of payment.

The original policy concerns that informed parts of the MiCA framework were closely linked to large-scale global stablecoin projects, such as Libra/Diem, which were intended to function as alternative payment instruments. To date, this use case has not materialised in practice.

At the same time, the FMA observes continuing market interest in certain ART structures, particularly commodity-linked tokens, including gold-linked arrangements. In such cases, the principal motivation of holders is generally exposure to the referenced asset and preservation of value rather than the use of the token for day-to-day payments.

The absence of authorised ARTs should therefore not necessarily be interpreted as evidence that there is no demand for ARTs. Rather, it may reflect the significant legal, regulatory and structuring challenges associated with developing ARTs that can be clearly distinguished from financial instruments, commodity-backed investment products or alternative investment funds.

The FMA therefore considers that a viable future role for ARTs is more likely to be found in the area of asset-backed and commodity-linked tokenisation than in the development of alternative payment instruments. If the European Commission intends ARTs to form a meaningful component of the EU crypto-

asset framework, further clarification of the boundaries between ARTs, financial instruments and investment funds at Level 1 would significantly support their practical development.

2.3. Liquidity and reserve requirements

Question 14. MiCA requires issuers of ARTs to establish, maintain, and prudently manage a reserve of assets and appropriate liquidity arrangements to ensure orderly redemptions and mitigate financial stability, liquidity, and operational risks. Additional and enhanced requirements apply to ARTs classified as “significant” under Article 45.

How do you think, if at all, each of the following elements of the MiCA liquidity and reserve regime for ARTs should be adjusted?

Please rate each aspect on a scale from 1 to 5, where

- “1” indicates that requirements should be significantly relaxed (e.g. lower liquidity buffers or remove specific obligations)
- “3” indicates that the current framework is appropriate and should remain unchanged
- “5” indicates that requirements should be made substantially more stringent (e.g. higher reserves, tighter risk controls, or enhanced safeguards)

a) Please rate each aspect below as regard to non-significant ARTs:

	1 (should be significantly relaxed)	2 (should be somehow relaxed)	3 (current framework appropriate)	4 (should be made somehow more stringent)	5 (should be made substantially more stringent)	Don't know - No opinion - Not applicable
Obligation to constitute and maintain a reserve of assets covering redemption and liquidity risks	☐	☐	☒	☐	☐	☐
Liquidity composition and maturity structure of the reserve (Article 36(4), RTS)	☐	☒	☐	☐	☐	☐
Minimum amount of deposits held (30% and 60%) (Article 36(4), RTS)	☐	☐	☒	☐	☐	☐
Auditing requirements (Article 36(9))	☐	☐	☐	☒	☐	☐
Custody requirements (Article 37)	☐	☐	☒	☐	☐	☐

b) Please rate each aspect below as regard to requirements for significant ARTs:

	1 (should be significantly relaxed)	2 (should be somehow relaxed)	3 (current framework appropriate)	4 (should be made somehow more)	5 (should be made substantially)	Don't know - No opinion - Not applicable

				stringent)	more stringent)	
Obligation to constitute and maintain a reserve of assets covering redemption and liquidity risks	☐	☐	☐	☐	☐	☐
Liquidity composition and maturity structure of the reserve (Article 36(4), RTS)	☐	☐	☐	☐	☐	☐
Minimum amount of deposits held (30% and 60%) (Article 36(4), RTS)	☐	☐	☐	☐	☐	☐
Auditing requirements (Article 36(9))	☐	☐	☐	☐	☐	☐
Custody requirements (Article 37)	☐	☐	☐	☐	☐	☐
Enhanced liquidity management, stress testing, monitoring, and reporting obligations for significant ARTs (Article 45(3)-(4))	☐	☐	☐	☐	☐	☐

Please explain your answers to question 14 a) and b), including your reasoning and any suggestions for recalibration or alternative approaches (e.g. greater risk sensitivity, differentiation by business model, or interaction with reserve and liquidity requirements):

The requirement of protection against insolvency of the reserve assets in the interests of investors is in practice almost impossible to implement. MiCAR does not establish any specific legal framework that ensure protection against insolvency and that at the same time allow the issuer to make use of the assets of the reserve of assets in case of liquidity mismatches (art 36 para 2 MiCAR). By contrast, the AIFMD provides for a segregated fund (Sondervermögen), while the EU-Covered Bond Directive provides for the creation of a cover pool. MiCAR contains no comparable mechanism. It should be further clarified whether the protection of the ART-holders' claims in case of insolvency of the issuer is prescribed ex lege through Art 36 para 2 MiCAR, or whether the issuer is merely required to separate the assets from its own estate (acc to Art 36 para 3 MiCAR). It is entirely unnecessary to state that the assets are held in the interests of the token holders (Art 36 para 2 MiCAR).

Art 37 para 1 letter a, which prescribes that the assets of the reserve of assets may not be pledged should be reevaluate, as this provision is in contradiction with the obligation to separate the assets from its own estate (Art 36 para 2 MiCAR). In legal systems that do not recognize segregated estates outside the cases expressly provided for by law, there is no other way to achieve a protection against insolvency than a pledged or a collateral arrangement. For example, it could be clarified that the assets may not be pledged in favour of third parties, while pledging the assets of the reserve of assets for the benefit of token holders should remain possible.

A stronger linkage between token holders and the reserve of assets may further blur the distinction between ARTs and alternative investment funds. In practice, one of the key challenges encountered in potential ART structures is that the reserve of assets often consists of the same assets that determine the value of the token. Where token holders are perceived as having rights that are closely linked to, or effectively limited by, the performance and availability of the reserve assets, the distinction from collective investment structures becomes increasingly difficult. The FMA therefore considers that any future review of MiCA should also address the boundary between ARTs and investment funds.

Question 15. MiCA sets out liquidity and reserve requirements for issuers of EMTs to ensure immediate redemption of tokens, mitigation of credit and operational risk, and resilience under stress scenarios. Additional requirements apply to EMTs classified as “significant” (Article 56). Should any of the following aspects of the MiCA regime for EMTs issued by e-money institutions be adjusted?

Please rate each aspect on a scale from 1 to 5, where

- “1” indicates that requirements should be significantly relaxed (e.g. lower liquidity buffers or remove specific obligations)
- “3” indicates that the current framework is appropriate and should remain unchanged
- “5” indicates that requirements should be made substantially more stringent (e.g. higher reserves, tighter risk controls, or enhanced safeguards)

a) Please rate each aspect below as regard to requirements for non-significant ARTs:

	1 (should be significantly relaxed)	2 (should be somehow relaxed)	3 (current framework appropriate)	4 (should be made somehow more stringent)	5 (should be made substantially more stringent)	Don't know - No opinion - Not applicable
Obligation to constitute and maintain a reserve of assets covering redemption and liquidity risks (Article 36(1))	☐	☐	☒	☐	☐	☐
Legal and operational segregation of reserve assets from the issuer's own estate and from other token reserves (Article 36(2) – (3))	☐	☐	☐	☒	☐	☐
Liquidity composition and maturity structure of the reserve (Article 36 (4), RTS)	☐	☐	☒	☐	☐	☐
Minimum amount of deposits held (30% and 60%) (Article 36(4), RTS)	☐	☐	☒	☐	☐	☐
Auditing requirements (Article 36(9))	☐	☐	☐	☒	☐	☐
Custody requirements (Article 37)	☐	☐	☒	☐	☐	☐
Excessive exposure / concentration between bank and token (Article 36(4) MiCA) Do you consider the 1.5% binding limit adequate? (RTS)	☐	☐	☒	☐	☐	☐

b) Please rate each aspect below as regard to requirements for significant ARTs:

	1 (should be significantly relaxed)	2 (should be somehow relaxed)	3 (current framework appropriate)	4 (should be made somehow more stringent)	5 (should be made substantially more stringent)	Don't know - No opinion - Not applicable
Obligation to constitute and maintain a reserve of assets covering redemption and liquidity risks (Article 36(1))	☐	☐	☒	☐	☐	☐
Legal and operational segregation of reserve assets from the issuer's own estate and from other token reserves (Article 36(2)–(3))	☐	☐	☒	☐	☐	☐
Liquidity composition and maturity structure of the reserve (Article 36 (4), RTS)	☐	☐	☒	☐	☐	☐
Minimum amount of deposits held (30% and 60%) (Article 36(4), RTS)	☐	☐	☒	☐	☐	☐
Auditing requirements (Article 36(9))	☐	☐	☒	☐	☐	☐
Custody requirements (Article 37)	☐	☐	☒	☐	☐	☐
Enhanced liquidity management, stress testing, monitoring, and reporting obligations for significant EMTs (Article 45(3)-(4))	☐	☐	☒	☐	☐	☐
Excessive exposure / concentration between bank and token (Article 36(4) MiCA) Do you consider the 1.5% binding limit adequate? (RTS)	☐	☐	☒	☐	☐	☐

Please explain your answers to question 15 a) and b), including your reasoning and any suggestions for recalibration or alternative approaches:

At the same time, the FMA considers that the current Level 1 framework may not provide sufficient legal certainty regarding the liquidity profile that reserve assets are expected to maintain. While MiCA establishes quantitative requirements regarding the proportion of reserve assets to be held as deposits, the more risk-sensitive aspects of liquidity management, including maturity limitations and liquidity buckets, are largely specified at Level 2.

From a prudential perspective, the maturity and liquidity requirements developed in the EBA RTS appear well suited to ensuring that reserve assets remain available to meet redemption requests under both normal and stressed conditions. These requirements may in some respects provide a more risk-sensitive framework than a simple fixed percentage requirement for deposits.

The FMA therefore considers that, as part of any future review, the European Commission could assess whether the key principles regarding reserve liquidity should be reflected more directly in Level 1. In particular, consideration could be given to whether both approaches:

- a minimum proportion of reserve assets held in deposits; and
- minimum liquidity and maturity requirements for the reserve as a whole,

should be explicitly recognised within the primary legislative framework of Level 1.

This could strengthen legal certainty, improve the transparency of the regime and ensure that the core prudential objectives of the reserve framework are anchored directly in MiCA rather than relying predominantly on Level 2 measures.

The FMA does not, at this stage, advocate a reduction of the existing deposit requirements. However, if the European Commission were to consider such a reduction in the future, it would be essential to ensure that robust Level 1 liquidity and maturity requirements remain in place to preserve the ability of issuers to meet redemption requests at all times.

The FMA further notes that the current interaction between MiCA and the E-Money Directive gives rise to unnecessary complexity and may create uncertainty regarding the applicable reserve framework for EMT issuers that are authorised as electronic money institutions.

In particular, the more detailed reserve of assets requirements under MiCA for ARTs are not applied uniformly to all EMTs. Certain enhanced requirements become applicable only in the case of significant EMTs issued by electronic money institutions, while non-significant EMTs remain subject to a combination of MiCA provisions and safeguarding requirements under the E-Money Directive.

While the EMD safeguarding framework provides an important layer of protection, the resulting interplay between two legislative regimes may create interpretative challenges and increases the risk of regulatory gaps, overlaps or inconsistent supervisory outcomes.

From the perspective of legal certainty and supervisory consistency, the European Commission could therefore assess whether the reserve of assets framework applicable to ARTs should serve as a more harmonised basis for EMT reserve requirements as well (and not just for sEMT issued by an EMI). A more uniform prudential framework across ARTs and EMTs could simplify the regulatory architecture, reduce complexity arising from the interaction of MiCA and the EMD, and minimise the risk of unintended differences in treatment between functionally similar stablecoin arrangements.

Such an approach would also improve transparency for issuers, token holders and competent authorities by ensuring that the core rules governing reserve composition, liquidity management and asset segregation are contained within a single legislative framework.

Question 16. Under MiCA, credit institutions issuing EMTs are not subject to the reserve asset segregation requirements or the requirement to maintain a reserve of assets applicable to non-bank EMT issuers (Article 58 MiCA). This is consistent with the approach to the regulation of traditional e-money.

Should MiCA be adjusted to introduce a requirement to maintain a reserve of assets and segregation requirements for reserve assets of EMTs issued by credit institutions?

- ☒ Yes – require reserve maintenance and segregation of EMT reserve assets within the credit institution's balance sheet
- ☐ Yes – require issuance through a legally separate entity of the credit institution with full segregation of EMT reserve assets
- ☐ No – keep the current MiCA approach unchanged
- ☐ Others / alternative approach
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 16, including your reasoning and any suggestions for other/alternative approaches:

Equal Treatment and Functional Equivalence

The FMA does not consider the reference to technological neutrality (as indicated by EBA and ECB) and the existing prudential framework for credit institutions to be sufficient justification for the absence of reserve segregation requirements for EMTs issued by credit institutions.

From an economic perspective, ARTs, EMTs issued by EMIs and EMTs issued by credit institutions perform essentially the same function, namely maintaining confidence in redeemability through assets backing the token. It is therefore difficult to justify why strict reserve segregation requirements apply to ARTs (issued by CI) and to EMTs issued by (s)EMIs, while comparable EMTs issued by credit institutions are exempt from such requirements.

The current framework therefore raises questions regarding the equal treatment of functionally equivalent stablecoin arrangements and may result in different regulatory outcomes for products with substantially similar economic characteristics.

Purpose of Reserve Segregation and Investor Protection

The FMA considers that one of the primary objectives of the reserve framework is to ensure that token holders benefit from a clearly identifiable and ring-fenced pool of assets, including in insolvency scenarios.

This objective remains relevant irrespective of whether the issuer is a credit institution or an electronic money institution. The prudential soundness of the issuer and the protection afforded to token holders in insolvency are distinct policy objectives.

Under the current framework, holders of EMTs issued by EMIs benefit from a more clearly protected and segregated reserve structure, whereas holders of EMTs issued by credit institutions may ultimately rank alongside other unsecured creditors. This creates a potential protection gap and may lead to materially different outcomes for token holders depending solely on the regulatory status of the issuer.

The FMA therefore considers that the current approach may result in a lower level of protection for holders of EMTs issued by credit institutions, which appears difficult to reconcile with MiCAR's broader investor protection objectives.

Interaction with Prudential Requirements

The FMA acknowledges the concerns regarding possible interactions with the Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR), including the risk of double counting.

However, such issues appear capable of being addressed through appropriate technical calibrations and adjustments to the prudential framework. Potential interactions with the LCR or NSFR should not, in themselves, constitute a decisive argument against reserve segregation if such segregation is considered necessary to achieve the underlying investor protection objectives of MiCAR.

Possible Future Review

The European Commission should assess whether reserve segregation requirements should apply consistently across all EMT issuers, irrespective of their authorisation status.

More generally, the FMA considers that the regulatory treatment should focus on the economic function of the token rather than the legal status of the issuer. Where crypto-assets perform the same stabilisation and redemption function, there should be a strong presumption in favour of equivalent reserve, segregation and investor protection requirements unless there is a clear policy justification for differentiated treatment.

2.4. Criteria for determining significance

Under MiCA, ARTs and EMTs may be classified as “significant” based on a set of quantitative and qualitative criteria set out in Article 43 (ARTs) and Article 56 (EMTs), which trigger enhanced prudential, governance, and supervisory requirements. The Commission has adopted a [delegated act](#) to further clarify the criteria for determining significance.

Question 17. Do you think the following quantitative criteria thresholds used to classify EMTs or ARTs as “significant” should be adjusted, and if so how?

Please rate each quantitative criteria thresholds on a scale from 1 to 5, where

- “1” = Significantly decreased (thresholds should be much lower / classification triggered earlier)
- “2” = Somewhat decreased
- “3” = Kept as is (current MiCA thresholds are broadly appropriate)
- “4” = Somewhat increased
- “5” = Significantly increased (thresholds should be much higher / classification triggered later)

a) Please rate how each quantitative criteria thresholds used to classify EMTs should be adjusted:

(	1 (significantly decreased)	2 (somewhat decreased)	3 (kept as is)	4 (Somewhat increased)	5 (significantly increased)	Don't know - No opinion - Not applicable
Number of holders / users exceeding 10 million (Articles 43 (1)(a) and 56)	☐	☐	☒	☐	☐	☐
Total outstanding value / market capitalisation exceeding EUR 5 billion (Articles 43 (1)(b) and 56)	☐	☐	☒	☐	☐	☐
Transaction volume or value per day (average 2.5 million transactions and EUR 500 million) (Articles 43 (1)(c) and 54)	☐	☐	☒	☐	☐	☐

b) Please rate how each quantitative criteria thresholds used to classify ARTs should be adjusted:

(	1 (significantly decreased)	2 (somewhat decreased)	3 (kept as is)	4 (Somewhat increased)	5 (significantly increased)	Don't know - No opinion - Not applicable
Number of holders / users exceeding 10 million (Articles 43 (1)(a) and 56)	☐	☐	☒	☐	☐	☐
Total outstanding value / market capitalisation exceeding EUR 5 billion (Articles 43 (1)(b) and 56)	☐	☐	☒	☐	☐	☐
Transaction volume or value per day (average 2.5 million transactions and EUR 500 million) (Articles 43 (1)(c) and 54)	☐	☐	☒	☐	☐	☐

Please explain your answers to question 17 a) & b), including your reasoning and any suggestions for other/alternative approaches:

Question 18. Do you think the qualitative criteria used to classify EMTs or ARTs as “significant” under MiCA should be adjusted?

- ☒ Yes
- ☒ No
- ☐ Don't know / no opinion / not applicable

Please explain how you think the qualitative criteria for classifying EMTs or ARTs as “significant” should be adjusted:

Please explain your answer to question 18:

Question 19. Are there any additional criteria or metrics that should be added to determine “significant” tokens?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please specify which criteria or metrics and explain why:

The FMA considers that participation in a third-country multi-issuance stablecoin arrangement should, as a matter of principle, not be regarded as compatible with the objectives of MiCA unless an appropriate regulatory framework is established.

However, should the European Commission decide to permit such arrangements, and in the absence of a robust equivalence regime for the relevant third-country framework, participation in a multi-issuer stablecoin scheme should constitute an additional criterion when assessing significance.

Multi-issuer arrangements give rise to specific risks that are not adequately captured by the existing significance criteria, including reserve fragmentation, cross-border redemption dynamics, regulatory arbitrage, supervisory complexity and increased contagion risk. These risks may become material irrespective of the size of the EU issuer's standalone issuance activity.

The FMA therefore considers that participation in a third-country multi-issuer stablecoin arrangement should be included as a factor in the significance assessment framework. This would ensure enhanced supervisory scrutiny and provide competent authorities and the EBA with appropriate tools to address the additional prudential and financial stability risks associated with such structures.

Any consideration of such a criterion should be closely linked to the broader assessment of the permissibility of third-country multi-issuer arrangements and the possible introduction of an equivalence framework, as recommended by the ESRB.

Please explain your answer to question 19:

2.5. Interest payment

MiCA currently prohibits the granting of interest or any interest-equivalent remuneration of stablecoins by either the issuer, offeror or crypto asset service provider. This prohibition applies to ARTs under Article 40 and to EMTs under Article 50 of MiCA.

Question 20. In your view, should the MiCA prohibition on granting interest or any interest-equivalent remuneration be modified?

a) for EMTs:

- ☒ No, interest and interest-equivalent remuneration should continue to be prohibited
- ☐ Yes, interest or interest-equivalent remuneration should be allowed under defined conditions
- ☐ Yes, interest or interest-equivalent remuneration should be allowed fully
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 20 a):

The FMA supports maintaining the current prohibition on granting interest or any interest-equivalent remuneration in relation to EMTs.

Allowing EMT issuers to pay interest would fundamentally alter the economic nature of the instrument. EMTs are intended to function primarily as means of payment and stores of value. The payment of interest would introduce a clear investment component and could call into question whether such products should continue to be classified as EMTs under MiCA or whether they would be more appropriately treated as investment products.

The FMA further considers that permitting interest would significantly complicate the distinction between EMTs and other regulated products, including deposits. One of the key objectives of MiCA is to establish clear boundaries between crypto-asset categories and existing financial services legislation. Introducing interest-bearing EMTs would increase similarities with traditional deposit products and could create additional legal uncertainty regarding the distinction between EMTs, deposits and other interest-bearing financial instruments.

Maintaining the current prohibition therefore supports regulatory clarity and preserves the distinct role of EMTs within the MiCA framework. The FMA does not see a need to modify the existing approach at this stage.

Please explain why you think interest or interest-equivalent remuneration should be allowed for EMTs, (including any benefits and risks) and specify the conditions under which it should be permitted:

b) for ARTs:

- ☒ No, interest and interest-equivalent remuneration should continue to be prohibited

- ☐ Yes, interest or interest-equivalent remuneration should be allowed under defined conditions
- ☐ Yes, interest or interest-equivalent remuneration should be allowed fully
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 20 b):

Same as above for EMTs

Please explain why you think interest or interest-equivalent remuneration should be allowed for ARTs, (including any benefits and risks) and specify the conditions under which it should be permitted:

2.6. Redemption

MiCA establishes distinct redemption regimes for ARTs and EMTs. For ARTs, redemption rights are primarily governed by Article 39, supported by operational and prudential requirements in Articles 36–38 and 47. For EMTs, redemption rights are set out in Article 49, with supporting provisions in Articles 46 and 47.

Question 21. Based on your experience either as a holder of EMTs or as an issuer of EMTs, how have redemption requests been processed and executed in practice by issuers or their agents? What practical problems, if any, have been encountered?

Question 22. If you hold EMTs and wish to dispose of them, which of the following options would you most likely choose?

a) In a normal market situation

- ☐ I would likely spend them (e.g. on goods or services)
- ☐ I would likely sell or exchange them with a broker or at a trading venue
- ☐ I would likely turn to the EMT issuer or his agent to exercise my statutory redemption right
- ☐ Don't know / no opinion / not applicable

b) In a stressed market situation

- ☐ I would likely spend them (e.g. on goods or services)
- ☐ I would likely sell or exchange them with a broker or at a trading venue
- ☐ I would likely turn to the EMT issuer or his agent to exercise my statutory redemption right
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 22 a) and b):

Question 23. For each of the redemption rights and rules listed below, please indicate whether the existing MiCA rules should be amended or specified or kept as they are.

Please consider, in particular, implications for financial stability, consumer protection, and cross-border usability.

	Weaken	Keep as is	Strengthen	Don't know - No opinion - Not applicable
Permanent right of redemption against the issuer, either at market value (ARTs) or at par (EMTs)	☐	☒	☐	☐
Timing of redemption (timeframe for redemption by the issuer)	☐	☐	☒	☐
Prohibition of redemption fees	☒	☐	☐	☐
Conditions, procedures, and transparency of redemption policies	☐	☒	☐	☐
Supervisory powers to intervene in or trigger redemption plans	☐	☒	☐	☐

Please explain your assessment to question 23, including if a different approach is warranted for significant vs non-significant tokens, or in crisis scenarios and share any suggestions for adjustments you may have:

The FMA generally supports the strong redemption rights framework established under MiCA, including the permanent right of redemption.

However, the FMA notes a potential tension between the prudential expectations imposed on issuers and the limited revenue opportunities available under the current framework.

In particular, MiCA requires reserve assets to be invested predominantly in highly liquid and low-risk assets. While these requirements are appropriate from a liquidity and investor protection perspective, they also inherently limit the returns that issuers can generate from reserve management activities.

In supervisory practice, questions frequently arise regarding the long-term sustainability of stablecoin business models, the plausibility of revenue projections and the issuer's ability to generate own funds through ongoing operations. At the same time, redemption rights are a core feature of MiCA and should not be weakened solely to enhance profitability.

At the same time, the FMA notes that the current framework already significantly restricts the revenue opportunities available to EMT issuers. In this context, the European Commission could consider whether redemption fees should remain permissible as a legitimate source of income, subject to appropriate safeguards.

It should also be noted that EMTs are typically traded on secondary markets and are not generally redeemed directly with the issuer on a frequent basis. As a result, redemption fees are unlikely to become the primary source of revenue for issuers. However, they may provide a limited and comparatively low-risk source of income which could contribute to the viability of EMT business models.

To prevent excessive costs for token holders and ensure fair treatment, consideration could be given to introducing reasonable limits or caps on redemption fees. Such an approach could support sustainable business models while preserving consumer protection objectives and the role of EMTs as payment instruments rather than investment products.

2.7 Stability issues

Stablecoins have the potential to reshape part of the financial service value chain as they can offer faster, cheaper, and more direct global payment and settlement transactions by bypassing certain financial intermediaries. They can also pose risks. This subsection aims to explore the adequacy of the safeguards provided by MiCA, especially regarding redemption and resolution plans.

Question 24. Articles 46 and 47 require issuers of ARTs and EMT to prepare a recovery plan and a redemption plan in case an issuer cannot comply with reserve requirements e.g. due to significant and sudden requests for redemptions.

Please indicate whether the current MiCA requirements are fit for purpose in those regards or should be amended:

a) Current MiCA requirements for ARTs

	Weaken	Keep as is	Strengthen	Don't know - No opinion - Not applicable
Recovery plans	☐	☐	☒	☐
Redemption plans	☐	☒	☐	☐

b) Current MiCA requirements for EMTs

	Weaken	Keep as is	Strengthen	Don't know - No opinion - Not applicable
Recovery plans	☐	☒	☐	☐
Redemption plans	☐	☒	☐	☐

Please explain your assessment to question 24 a) & b), including if a different approach is warranted for significant vs non-significant tokens, and share any suggestions for adjustments you may have:

Recovery Plans as Part of the Authorisation Process

The FMA considers that the current timing of the recovery plan requirement under Article 46(2) MiCA should be reassessed.

Under the current framework, issuers are required to submit the recovery plan within six months after authorisation or approval of the crypto-asset white paper. While this approach may reduce the burden during the authorisation phase, it also means that competent authorities only assess a key prudential safeguard after the issuer has already been authorised.

From a supervisory perspective, recovery planning should be an integral part of the authorisation process. The recovery plan provides important information

regarding the issuer's ability to respond to stress events, liquidity pressures, reserve shortfalls and operational disruptions. These considerations are highly relevant when assessing the overall viability and resilience of the proposed business model.

Where material weaknesses are identified only after authorisation has been granted, supervisory options may be more limited and remediation may be more difficult than if such issues had been identified during the initial assessment.

The FMA therefore considers that the European Commission should assess whether recovery plans should form part of the authorisation process rather than being submitted after authorisation. This would allow competent authorities to evaluate the issuer's recovery capabilities, governance arrangements and contingency measures as part of the overall licensing assessment and could contribute to a more robust prudential framework.

Question 25. EMTs issued by authorised e-money institutions (EMIs) could potentially operate with enhanced monetary and financial safeguards.

Please rate the appropriateness and desirability of the following policy options for EMTs issued by e-money institutions:

	1 (not at all appropriate / desirable)	2 (slightly appropriate / desirable)	3 (moderately appropriate / desirable)	4 (mostly appropriate / desirable)	5 (highly appropriate / desirable)	Don't know - No opinion - Not applicable
Allowing EMT issuers to deposit their reserve assets directly into central bank accounts	☐	☐	☐	☐	☐	☒
Providing clear rules that ensure the continuity of redemption rights (reserves are safeguarded for the benefit of token holders and are ring-fenced in insolvency, giving exclusive claim against those assets) in case of insolvency of the issuer	☐	☐	☐	☐	☒	☐
Establishing a dedicated resolution regime for EMIs issuing EMTs	☐	☐	☐	☐	☐	☒
Allowing emergency liquidity support / lender-of-last-resort (LOLR) facilities for EMIs issuing EMTs	☐	☐	☒	☐	☐	☐
Others	☐	☐	☐	☐	☐	☒

Please specify to what other policy option(s) you refer in your answer to question 25:

Please explain your ratings in question 25, including potential benefits, risks, or implementation challenges:

The FMA supports the objective that reserve assets should remain protected in the event of the issuer's insolvency. However, practical experience has

highlighted legal uncertainty regarding the precise effect of Article 36(2) MiCA.

In particular, it remains unclear whether MiCA itself is intended to ensure insolvency protection of reserve assets as a matter of EU law or whether issuers are merely required to achieve such protection through arrangements available under the applicable national legal framework.

This distinction is important, as the legal mechanisms available to ensure insolvency remoteness differ across Member States. Moreover, the specific legal arrangements chosen to achieve segregation and insolvency protection may have implications for the regulatory classification of the structure, including in relation to investment fund legislation.

The European Commission should therefore clarify the intended legal effect of Article 36(2) MiCA and the interaction between MiCA reserve requirements and national insolvency laws. Greater clarity would enhance legal certainty, promote supervisory convergence and reduce classification challenges in practice.

Question 26. How appropriate is it to require EMT-issuing EMIs to hold 30-60% of their reserve assets in bank deposits?

- ☐ 1 - Not at all appropriate / desirable
- ☐ 2 - Slightly appropriate / desirable
- ☐ 3 - Moderately appropriate / desirable
- ☐ 4 - Mostly appropriate / desirable
- ☒ 5 - Highly appropriate / desirable
- ☐ Don't know / no opinion / not applicable

Please explain your ratings in question 26 and add any suggestions for recalibration or alternative approaches:

See also Q 15: The FMA considers the current requirement for EMT-issuing EMIs to hold 30% (and 60% for significant EMTs) of reserve assets in the form of deposits to be appropriate and should be maintained at this stage.

The requirement provides a clear and easily applicable prudential safeguard that supports liquidity and redemption capacity. Given the limited supervisory experience acquired to date, the FMA does not currently see sufficient evidence to justify a reduction or removal of the deposit requirement.

At the same time, the FMA recognises the value of the more risk-sensitive liquidity framework developed in the EBA RTS, including the maturity and liquidity requirements applicable to reserve assets. These requirements contribute significantly to ensuring that reserve assets remain available to meet redemption requests under both normal and stressed conditions.

Rather than replacing the current deposit requirement, the European Commission could consider whether key liquidity and maturity principles should be reflected more directly in Level 1 legislation. A combination of minimum deposit holdings and risk-sensitive liquidity requirements may provide a more robust and legally certain framework than relying exclusively on either approach.

The FMA therefore does not support removing the existing deposit requirement at this stage. Any future review should carefully assess whether additional Level 1 recognition of maturity and liquidity requirements would further strengthen the framework while preserving the simplicity and prudential benefits of the current deposit-based safeguard.

2.8. Global stablecoins arrangements and interactions with other regulatory frameworks

Global stablecoins are stablecoins that have a wide existing or potential reach and use across multiple jurisdictions.

Question 27. What are the potential benefits of global stablecoins for different use cases?

For each use case below, please indicate on a scale of 1 to 5 how beneficial global stablecoins would be for EU holders:

	1 (not beneficial)	2 (moderately beneficial)	3 (neutral)	4 (rather beneficial)	5 (very beneficial)	Don't know - No opinion - Not applicable
International payments (cross-border remittances or transfers,)	☐	☐	☐	☒	☐	☐
Intra-EU payments (domestic and cross-border EU payments)	☐	☒	☐	☐	☐	☐
Crypto trading and liquidity provision	☐	☐	☐	☒	☐	☐
Retail payments - Person to Person	☐	☒	☐	☐	☐	☐
Retail payments - Person to Business (POI payment to merchants including e-commerce)	☐	☒	☐	☐	☐	☐
Retail payments - Business to Business	☐	☒	☐	☐	☐	☐
Settlement of tokenised financial instruments (e. g., digital bonds, securities)	☐	☐	☐	☒	☐	☐
Corporate treasury management	☐	☐	☒	☐	☐	☐
Access to programmable or smart contract-based financial services (DeFi applications)	☐	☐	☐	☒	☐	☐
Provision of financial services in underserved regions in the world	☐	☐	☐	☐	☒	☐
Other potential use cases	☐	☐	☐	☐	☐	☒

Please specify to what other potential use case(s) you refer in your answer to question 27:

Please explain your answers to question 27:

The FMA generally agrees that global stablecoins may provide benefits in certain cross-border and crypto-asset related use cases. In particular, they may facilitate international transfers where existing payment infrastructures are inefficient, expensive or inaccessible.

However, the FMA considers that the benefits for intra-EU payments are likely to remain limited. The EU already benefits from highly efficient payment infrastructures, including SEPA Instant and ongoing Eurosystem initiatives aimed at enabling DLT-based settlement using central bank money. As a result, privately issued global stablecoins currently have limited incentives to displace existing payment and settlement solutions within the Union.

The FMA also considers that the benefits of stablecoins in tokenised financial markets remain uncertain. While stablecoins may facilitate settlement in certain DLT-based environments, the ongoing development of central bank money solutions for DLT-based settlement may reduce the long-term need for privately issued settlement assets.

At the same time, the FMA acknowledges that stablecoins may provide greater benefits in jurisdictions characterised by limited access to banking services, weak domestic currencies or high inflation. These factors may explain increasing adoption in certain emerging markets. However, such conditions are generally not present in the EU financial system.

Overall, the FMA considers that stablecoins are likely to remain concentrated in niche use cases, particularly within the crypto-asset ecosystem and selected cross-border applications. The long-term sustainability of stablecoins as a broadly adopted payment instrument remains uncertain, especially given competition from existing payment infrastructures and ongoing public-sector initiatives in the area of digital settlement and tokenised financial markets

Question 28. How important is it for EU users (both people and businesses) to be able to access global stablecoins via EU-based and licenced issuers and CASPs?

	1 (not important at all)	2 (moderately important)	3 (neutral / no clear preference)	4 (rather important)	5 (highly important)	Don't know - No opinion - Not applicable
EU-based and licenced stablecoins Issuers	☐	☐	☐	☒	☐	☐
EU-based and licenced CASPs	☐	☐	☐	☐	☒	☐

Please explain your answers to question 28:

Crypto-asset markets are inherently global, while liquidity available within the EU market remains more limited than in major global markets. Access to global stablecoins can therefore be important for EU users, particularly for accessing global trading pairs and liquidity pools, achieving efficient execution and avoiding market fragmentation. Excessively restricting such access could impair the competitiveness of EU-authorised CASPs and create incentives for EU users to migrate to non-EU providers or decentralised channels, where MiCAR safeguards and effective supervisory oversight may not apply.

However, access to global stablecoins should not be unconditional. In the absence of an issuer authorised and supervised under MiCAR, EU users cannot be assumed to benefit from rights and safeguards equivalent to those applicable to MiCAR-compliant ARTs or EMTs. Any framework for third-country

stablecoins should therefore focus on verifiable and enforceable safeguards, a clearly identified entity responsible towards EU users, and effective supervisory cooperation. Where such safeguards are not available, the stablecoin should not be offered, admitted to trading or actively marketed to EU users. EU-authorised CASPs can play an important role as regulated gateways by applying appropriate due diligence, disclosure, governance and customer-protection requirements.

Particular attention should be paid to preventing regulatory arbitrage and misleading perceptions regarding the regulatory status of the stablecoin or its issuer. The involvement of an EU-authorised CASP should not, by itself, imply that the underlying stablecoin or a third-country issuer is fully supervised under MiCAR. At the same time, regulatory safeguards should be designed in a proportionate manner that preserves access to global liquidity and avoids isolating the EU market from the global crypto-asset ecosystem.

Question 29. Based on your experience and assessment, how significant are the following risks associated with a multi-issuance model^[3] of global stablecoins for the EU financial system?

[3] Under a multi-issuer model, the global stablecoin issuer operates subject to the requirements of the EU MICA framework for stablecoins offered or held in the EU (EU establishment, EU reserve requirements, redemption obligations, EU supervision) and the requirements of third country jurisdictions, if any, where it also issues or offers stablecoins. Protection of EU holders relies on EU prudential, operational, and consumer protection safeguards set out in MICA.

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather significant)	5 (very significant)	Don't know - No opinion - Not applicable
Run risk and reserve depletion in the EU (e.g. cross-border migration of tokens during stress leading to sudden increase of redemption pressure on EU issuers)	☐	☐	☐	☐	☒	☐
Unbalanced reserve distribution across jurisdictions (e.g. fragmentation of reserves between EU and non-EU entities)	☐	☐	☐	☐	☒	☐
Cross-border reserve transfer restrictions (e.g. third-country limitations on moving reserves during stress events)	☐	☐	☐	☐	☒	☐
Regulatory arbitrage due to fungibility of tokens (e.g. operation across regimes exploiting differences in prudential or conduct rules)	☐	☐	☐	☐	☒	☐
Supervisory monitoring and data-tracking challenges (e.g. difficulty measuring EU-holdings, especially holdings in self-custodial wallets)	☐	☐	☐	☐	☒	☐
Risks resulting from the stablecoin issuer home jurisdictions not having prudential or conduct rules that	☐	☐	☐	☒	☐	☐

meet internationally accepted standards or that are significantly lower than those set out in EU law						
Others	☐	☐	☐	☐	☐	☒

Please specify to what other risk(s) you refer in your answer to question 29. Please elaborate:

Please explain the reasoning behind your ratings in question 29. Describe the nature and importance of these risks, the underlying assumptions, market dynamics, or regulatory factors informing your view:

The FMA considers run risk in third-country multi-issuer stablecoin arrangements to be significant.

Differing redemption conditions across participating issuers may incentivise token holders to direct redemption requests towards the most favourable issuer during periods of stress. This risk is particularly relevant where EU-regulated issuers are subject to stricter prudential and conduct requirements than third-country issuers. As MiCA does not limit redemption rights to EU-based holders, redemption pressure may arise from the broader global stablecoin ecosystem rather than only the EU issuer's customer base.

Consequently, redemption volumes could exceed normal expectations and create significant liquidity stress for the EU issuer, particularly where reserve assets are fragmented across multiple entities and jurisdictions. The FMA therefore considers run risk to be a key prudential concern.

The FMA also considers reserve fragmentation across jurisdictions to be a significant risk.

Available supervisory information suggests that reserves held by EU issuers often represent only a limited share of the reserves backing global stablecoin arrangements. In a stress scenario involving large-scale redemptions directed towards the EU issuer, effective reserve rebalancing across jurisdictions may therefore become critical.

However, the effectiveness of such arrangements is uncertain. Third-country authorities may be unwilling to permit substantial outflows of reserve assets during periods of stress, particularly where local investors or financial stability could be affected. Legal, operational and regulatory constraints may further impede the timely transfer of assets, even where contractual rebalancing arrangements exist.

The FMA therefore views reserve fragmentation as a structural vulnerability. In practice, the availability of reserves in the jurisdiction where redemption demand materialises may be more important than the theoretical existence of reserves elsewhere within the arrangement.

The FMA considers regulatory arbitrage to be another key risk.

Reserve rebalancing arrangements may encourage the allocation of reserve assets to jurisdictions with lighter regulatory requirements or higher yields. Where non-EU issuers are not subject to prudential standards equivalent to MiCA, reserve assets may increasingly be held outside the EU regulatory framework.

This could undermine MiCA's objective of ensuring that reserves are invested in sufficiently liquid and low-risk assets capable of supporting redemption requests under stressed conditions. Token fungibility further exacerbates this risk, as holders may not distinguish between different reserve structures, while issuers may have incentives to prioritise returns over prudential safeguards.

As a result, multi-issuer arrangements may facilitate the migration of reserves to lower-regulation environments while continuing to benefit from the credibility associated with EU-regulated issuers. The FMA therefore supports further consideration of mitigating measures, including a robust equivalence framework and the implementation of ESRB recommendations.

The FMA also considers supervisory monitoring and data-tracking challenges to be significant.

Relevant information may not be directly available to EU supervisors where reporting obligations do not apply to all participating issuers. Competent authorities may therefore have to rely primarily on information provided by the EU issuer, making it difficult to obtain a complete picture of the overall arrangement.

These limitations are particularly relevant for significance assessments, reserve adequacy assessments and liquidity risk monitoring. Effective supervision therefore requires enhanced transparency regarding global token supply, reserve distribution, redemption activity and relationships between participating issuers. Without such information, the assessment of prudential risks and the application of significance criteria may be materially impaired.

Question 30. MiCA does not currently prohibit multi-issuer models, nor does the EU have jurisdiction to determine how third country entities, that also have licensed entities in the EU, should be regulated in third country jurisdictions.

Given your assessment of the advantages or disadvantages of global stablecoins and multi-issuance models, do you think that MiCA should continue to be open to multi-issuance models?

- ☐ Yes, the multi-issuance model for stablecoins should be permitted under MiCA
- ☒ No, MiCA should disallow the multi-issuance model for stablecoins
- ☐ Don't know / no opinion / not applicable

Please explain the reasons for your response to question 30 and describe the potential implications for the EU market and relevant stakeholders:

The FMA considers that third-country multi-issuer stablecoin arrangements should, as a matter of principle, not be regarded as compatible with the current MiCA framework.

This view follows from the structure and objectives of MiCA itself. For ARTs, Article 16(1)(a) MiCA requires the issuer to be established in the Union. Similarly, EMT issuance is limited to authorised credit institutions and electronic money institutions, which are subject to EU supervision and regulatory requirements. The MiCA framework is therefore built around the principle that the issuer, the reserve assets, the redemption obligations and the supervisory responsibility are aligned within the EU regulatory perimeter.

The FMA also supports the concerns expressed by the ESRB regarding third-country multi-issuer stablecoin arrangements.

From a supervisory perspective, such arrangements create significant practical and prudential challenges. Effective supervision requires reliable information regarding total issuance, reserve composition, reserve allocation, redemption flows and risk concentrations. In a multi-issuer structure involving third-country entities, it may be difficult or impossible for EU authorities to obtain a complete and timely overview of the scheme as a whole. This may significantly impair supervisory effectiveness and risk assessment.

Moreover, the fragmentation of reserves and redemption obligations across multiple jurisdictions creates substantial enforcement and crisis-management challenges. During periods of stress, it may be unclear whether reserve assets are available where redemption demand arises and whether supervisory measures adopted by EU authorities can effectively address risks originating outside the Union.

Should the European Commission nevertheless decide to permit third-country multi-issuer arrangements, the FMA considers that this should only occur within a dedicated framework based on regulatory equivalence. In this regard, the equivalence approach reflected in the US GENIUS Act may provide a useful point of reference.

However, any such approach would require a clear EU mechanism for assessing whether third-country regimes provide prudential, supervisory and investor protection outcomes that are equivalent to those required under MiCA. It would also be necessary to determine which EU authority is responsible for conducting such equivalence assessments and for monitoring ongoing compliance.

Absent a robust equivalence framework, the FMA considers that third-country multi-issuer stablecoin arrangements would present material supervisory, prudential and financial stability risks that are impossible to reconcile with the objectives of MiCA.

Question 31. MiCA considers that all EMTs that are pegged to or denominated in an EU currency are offered to the EU and therefore fully subject to MiCA issuer requirements.

a) Does this approach continue to be justified in view of market developments?

- ☐ Yes
- ☐ No
- ☒ Don't know / no opinion / not applicable

b) Does it discourage the international role of the euro?

- ☐ Yes
- ☐ No
- ☒ Don't know / no opinion / not applicable

Please explain your answer to question 31 a) & b):

--

Question 32. What are the advantages and disadvantages of this approach for the EU and the international role of EU currencies?

--

2.9. Interaction with the EU's economic security and the international role of the euro

Question 33. To what extent do you believe that euro-denominated stablecoins can contribute to the following objectives?

	1 (not at all effective)	2 (slightly effective)	3 (moderately effective)	4 (rather effective)	5 (highly effective)	Don't know - No opinion - Not applicable
Strengthening EU payment autonomy in retail payments	☐	☒	☐	☐	☐	☐
Strengthening EU payment autonomy in wholesale payments	☐	☐	☒	☐	☐	☐
Enhancing the international role of the euro	☐	☐	☐	☒	☐	☐

Please explain your answers to question 33:

The FMA considers that euro-denominated stablecoins are only likely to make a limited contribution to EU payment autonomy in retail payments. The EU already benefits from highly efficient retail payment infrastructures, including SEPA Instant and a mature digital payments ecosystem. As a result, the incremental benefits of euro-denominated stablecoins in this area appear limited.

For wholesale payments, the potential benefits are somewhat greater, particularly in connection with tokenised financial markets and DLT-based settlement. However, the ultimate role of stablecoins remains uncertain given ongoing Eurosystem initiatives aimed at enabling DLT-based settlement using central bank money. Solutions such as Pontes, Appia and other interoperability arrangements may achieve similar objectives while preserving the role of central bank money at the core of the financial system.

The FMA sees the strongest potential contribution in relation to the international role of the euro. Euro-denominated stablecoins may facilitate the use of euro-denominated assets and payment instruments in digital and cross-border environments and could therefore support the international visibility and accessibility of the euro.

At the same time, the FMA considers that the long-term role of stablecoins remains uncertain. Current adoption continues to be concentrated in a relatively limited number of use cases, and it is not yet evident that stablecoins will become the preferred settlement asset in either retail or wholesale markets where efficient public and private alternatives already exist. Consequently, while euro-denominated stablecoins may support the international role of the euro to some extent, their contribution to EU payment autonomy is likely to remain more limited.

2.10. Current safeguards in MiCA

Question 34. MiCA provides safeguards to mitigate the risks of multi-issuance stablecoins.

For each safeguard listed below, please indicate how effective you consider it to be:

	1 (not at all effective)	2 (slightly effective)	3 (moderately effective)	4 (rather effective)	5 (highly effective)	Don't know - No opinion - Not applicable
Restriction of widely used ARTs and EMTs denominated in a currency that is not an official currency of a Member State (Articles 23, 58)	☐	☒	☐	☐	☐	☐
ECB binding opinion powers on withdrawing authorization and limit the amounts of ARTs and EMTs (Articles 24(2) (3), 58)	☐	☒	☐	☐	☐	☐
EU establishment requirement for ART and EMT issuers (Article 16)	☐	☒	☐	☐	☐	☐
Reserve location, composition and liquidity requirements for ARTs and EMTs (Articles 36-38, 45, 54)	☐	☒	☐	☐	☐	☐
The powers of competent authorities listed in Article 94, especially to suspend or prohibit the trading of crypto-assets	☐	☒	☐	☐	☐	☐
National supervisory intervention powers (Article 105)	☐	☒	☐	☐	☐	☐
EBA temporary intervention powers (Article 104)	☐	☒	☐	☐	☐	☐

Please explain your answers to question 34:

The FMA would recommend a rating of 2 (slightly effective) for these safeguards in the context of third-country multi-issuer stablecoin arrangements.

More fundamentally, the FMA questions whether many of these safeguards are capable of effectively addressing the risks arising from third-country multi-issuer schemes at all. The current MiCA framework was designed on the basis that the issuer is established in the Union and remains fully subject to EU prudential and supervisory requirements. Indeed, Article 16 MiCA requires ART issuers to be established in the Union and EMT issuance is restricted to authorised credit institutions and electronic money institutions operating within the EU regulatory framework.

In the FMA's view, third-country multi-issuer arrangements are difficult to reconcile with these principles and should generally not be regarded as permissible under the current MiCA framework. This view is also consistent with the concerns expressed by the ESRB.

Against this background, the effectiveness of the safeguards listed above is inherently limited. For example, the EU establishment requirement loses much of its practical value if material issuance, reserve management and redemption functions can ultimately be performed by non-EU entities participating in the same stablecoin arrangement.

Similarly, reserve location, composition and liquidity requirements may be circumvented in practice through reserve allocation and rebalancing mechanisms. Such mechanisms may incentivise reserves to be held in jurisdictions offering higher yields or less demanding prudential requirements, thereby creating significant opportunities for regulatory arbitrage.

The FMA also considers the ECB's powers to be of only limited effectiveness in this context. These powers become relevant primarily where risks to the monetary system or the euro have already reached a significant scale. However, the supervisory challenges associated with multi-issuer arrangements arise much earlier, including during authorisation and the build-up phase of the arrangement, when questions regarding reserves, redemption obligations, governance and supervisory access first emerge.

Likewise, intervention powers available to competent authorities, national authorities and the EBA may prove difficult to exercise effectively where material elements of the arrangement are located outside the EU regulatory perimeter.

The FMA therefore considers that the central issue is not the calibration of existing safeguards, but rather whether third-country multi-issuer stablecoin arrangements should be permitted in the first place. If the European Commission nevertheless wishes to allow such arrangements, a dedicated framework based on robust equivalence assessments and the implementation of the ESRB recommendations would be necessary. Without such a framework, the effectiveness of the existing MiCA safeguards remains limited.

Moreover, MiCAR provides product intervention powers to NCAs and the ESAs. However, MiCAR does not provide an explicit legal basis for market monitoring. It is therefore unclear whether and to what extent an ESA intends to carry out market monitoring. If an ESA were to do so, questions arise as to how such monitoring would be conducted in practice, particularly with regard to the identification of products that may warrant intervention measures and the data on which such monitoring would be based. An explicit legal framework for market monitoring would be desirable

Question 35. MiCA requires that the reserves of the EMTs and ARTs issued, offered or held in the EU should be held in the EU.

Can the tokens held in the EU be determined or estimated with sufficient accuracy and frequency?

- ☐ Yes, EU holdings can be determined with sufficient accuracy and frequency
- ☒ Partially, but with some limitations (e.g., delays, estimation challenges)
- ☐ No, current methods are insufficient for reliable compliance
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 35, including any specific remarks with regard to tokens held in unhosted wallets:

The FMA considers that tokens held in the EU can currently only be determined with limited accuracy and subject to important methodological constraints.

A key challenge is that the current reporting framework and the prudential requirements regarding reserve assets are not fully aligned. Under MiCA, the regulatory framework primarily focuses on the issuance and public offering of tokens in the EU, whereas significant parts of the available supervisory data relate to holdings maintained by EU-regulated CASPs in custody.

This creates uncertainty as to the relevant reference point for determining the reserve assets that should be maintained in the EU. In particular, it is not always clear whether reserves should correspond to:

- the volume of tokens originally offered to the public in the EU;
- the volume of tokens currently held by EU investors;
- the volume of tokens held in custody by EU-authorized CASPs; or
- the volume of tokens that may potentially be redeemed by EU holders.

These concepts may differ significantly in practice, particularly where tokens are freely transferable across jurisdictions and between hosted and unhosted wallets.

The FMA further notes that Article 3(1)(32) MiCA defines the reserve of assets by reference to the assets securing redemption obligations. This concept does not necessarily coincide with either the volume publicly offered in the EU or the volume currently held through EU intermediaries. As a result, uncertainty remains regarding the appropriate basis for determining reserve requirements and their territorial allocation.

For supervisory purposes, greater clarity would therefore be desirable regarding the relationship between issuance, EU holdings, custody data and redemption obligations. In particular, the European Commission should consider clarifying which metric should serve as the primary reference point for reserve requirements and whether additional reporting obligations on issuers may be necessary to ensure consistent and reliable monitoring.

The challenges are further amplified in relation to unhosted wallets, where holdings can generally only be estimated through indirect methods and blockchain analytics, thereby limiting supervisory certainty regarding the actual volume of tokens effectively held within the Union.

Question 36. Should MiCA redemption rights be explicitly limited to EU holders only?

☒ Yes

☐ No

☐ Don't know / no opinion / not applicable

Please explain your answer to question 36, specifying what criteria should be used to determine who qualifies as an EU holder, and providing a rationale for your proposed approach:

Please explain your answer to question 36:

The FMA supports limiting MiCA redemption rights to EU holders.

From a supervisory perspective, such an approach would significantly enhance legal certainty and reduce a number of practical challenges associated with cross-border issuance and redemption arrangements, particularly in the context of multi-issuer stablecoin schemes.

In particular, limiting redemption rights to EU holders would ensure a clearer alignment between the obligations of the EU issuer, the corresponding reserve assets and the holders protected by the MiCA framework. The EU issuer would only be required to maintain reserves corresponding to its obligations towards EU holders, thereby reducing uncertainties regarding reserve allocation, reserve rebalancing mechanisms and cross-border redemption flows.

The FMA further considers that such an approach would substantially improve supervisory monitoring and reporting. Competent authorities would no longer need to rely on global token distribution data or redemption dynamics involving entities outside the EU supervisory perimeter. Instead, reserve requirements and supervisory reporting could be calibrated directly against liabilities towards identifiable EU holders.

The FMA considers that an EU holder could, for example, be defined by reference to residence within the European Union. Such an approach would be operationally feasible for issuers, as residence information is already collected and verified as part of customer due diligence and onboarding processes. This would provide an objective and relatively straightforward criterion that can be applied consistently across Member States.

More generally, limiting redemption rights to EU holders would better align the scope of MiCA's prudential safeguards with the scope of EU supervisory powers. It would also address several of the practical challenges associated with third-country multi-issuer arrangements and reduce the need for complex cross-border reserve management and rebalancing arrangements. The FMA therefore considers that limiting redemption rights to EU holders would improve supervisory effectiveness, enhance legal certainty and contribute to a more coherent prudential framework.

2.11. Potential additional safeguards

Question 37. In a multi-issuance model, reserve assets may be located across jurisdictions and legal entities. Concerns have been expressed that in times of market stress, the transfer or rebalancing of reserves between issuers may be delayed or restricted.

Is this concern valid or substantiated in your view?

- ☒ Valid-substantiated
- ☐ Not valid-not substantiated
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 37:

see above

Question 38. How effective would the following possible additional measures be in mitigating such concerns?

	1 (highly ineffective)	2 (rather ineffective)	3 (neutral / uncertain)	4 (somewhat effective)	5 (highly effective)	Don't know - No opinion - Not applicable
Introducing requirements that would favour or strengthen the redemption rights of holders of stablecoins that are genuinely circulating in the EU, as opposed to redemption rights associated with stablecoins transferred to the EU in times of stress to take advantage of MiCA protections (including redemption rights)	☐	☐	☐	☒	☐	☐
Restricting direct redemption rights in the EU to holders who are clients of EU-authorized CASPs, while holders that keep the tokens in un-hosted wallets do not have a MiCA guaranteed redemption right in the EU.	☐	☐	☐	☐	☒	☐
Differentiating redemption rights in crisis situations between retail and wholesale/professional holders	☐	☒	☐	☐	☐	☐
Requiring a dedicated liquidity buffer or additional reserve tranche specifically calibrated to cover	☐	☒	☐	☐	☐	☐

short-term redemption spikes in the EU						
Strengthening real-time or high-frequency reserve and liquidity reporting to EU competent authorities, including granular disclosure of reserve location and transfer constraints	☐	☒	☐	☐	☐	☐
Establishing binding cooperation arrangements between home and host supervisors to ensure rapid approval and execution of cross-border reserve transfers in stress scenarios	☐	☐	☒	☐	☐	☐
Others	☐	☐	☐	☐	☐	☒

Please specify to what other possible additional measure(s) you refer in your answer to question 38:

Please explain your answers to question 38:

The FMA considers that the proposed measures vary significantly in their effectiveness.

The FMA broadly supports restricting direct redemption rights in the EU to holders that can be reliably identified as EU holders, for example through EU-authorized CASPs. This would help reduce the risk of non-EU holders redirecting redemption requests to EU issuers during periods of stress in order to benefit from MiCA protections and redemption conditions.

At the same time, the FMA notes that considerable challenges remain regarding the determination of tokens genuinely circulating within the EU. Current supervisory visibility is incomplete, as reporting is primarily available from authorised EU CASPs. Holdings maintained through non-EU platforms or intermediaries may not be visible to EU supervisors. As a result, the actual volume of tokens effectively held by EU investors may be difficult to determine with precision.

The FMA is less convinced by measures based solely on additional liquidity buffers or enhanced reporting obligations. While such measures may improve resilience and supervisory visibility, they do not address the underlying structural problem that reserve assets may need to be rebalanced across jurisdictions in a stress scenario. The practical ability to execute such transfers remains uncertain.

Similarly, enhanced reporting cannot fully resolve the issue where the relevant information is not available to EU authorities in the first place or where significant parts of the stablecoin arrangement remain outside the EU supervisory perimeter.

The FMA sees greater value in arrangements that strengthen supervisory cooperation and facilitate cross-border reserve management. However, the effectiveness of such arrangements will depend on their legal enforceability and their ability to operate effectively during periods of market stress. In particular, it remains uncertain whether jurisdictions experiencing financial stress would permit significant reserve transfers abroad where such transfers

may conflict with domestic financial stability considerations. Overall, the FMA considers that measures addressing redemption access and cross-border supervisory coordination are likely to be more effective than measures focusing solely on additional liquidity requirements or reporting, as the latter do not fully address the underlying challenges associated with fragmented reserve structures and cross-jurisdictional redemption dynamics.

Question 39. If you referred in your response to question 38 to adjusting redemption rights, please provide any comments on the operational feasibility, legal implications, proportionality, or potential intended or unintended consequences of such amendments the redemption rights in MiCA as listed above or in any other way:

See Q 36.

Question 40. Do you see merit in introducing an [equivalence regime](#) for global stablecoins in the EU?

- ☐ Yes but only if other mitigation measures are not introduced
- ☒ Yes, in addition to mitigation measures
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please provide reasons for your response to question 40, including any perceived advantages or disadvantages of equivalence regimes:

Only to a limited extent and subject to strict conditions. An equivalence regime could provide a structured framework for global stablecoins issued in third countries. However, it must not allow access to the EU market on the basis of materially lower standards than those applicable to ARTs and EMTs issued under MiCAR.

Equivalence should therefore not be based merely on formal similarities between legal frameworks. It would need to ensure substantively comparable regulatory and supervisory outcomes, particularly regarding reserve assets, liquidity management, governance, recovery and redemption arrangements. The rights of EU holders would have to be legally enforceable against a clearly identified entity, including under stress and insolvency conditions. EU authorities would also require timely access to all information necessary for effective supervision.

Particular caution is warranted because a third-country issuer would not be authorised and directly supervised under MiCAR. EU users therefore cannot be assumed to benefit from rights and safeguards equivalent to those applicable to MiCAR-compliant ARTs or EMTs. This is particularly relevant where reserves are held outside the EU, restrictions on cross-border asset transfers may apply, or responsibilities are distributed between several entities within a global group.

Any equivalence regime should therefore include:

- an outcome-based assessment of the third-country regulatory and supervisory framework;
- effective supervisory cooperation and information-sharing arrangements;
- a clearly identified entity legally responsible towards EU holders;

- enforceable redemption rights and adequate arrangements for reserve assets and liquidity;
- safeguards ensuring access to and transferability of reserve assets, including under stressed conditions;
- ongoing monitoring and the possibility to suspend or withdraw equivalence at short notice; and
- restrictions on EU market access where these requirements are not or no longer met.

Equivalence decisions should be taken centrally at EU level and should not grant an automatic right of market access solely based on a third-country authorisation. Depending on the scale and use of the stablecoin in the EU, additional requirements could remain necessary, such as EU representation, registration or specific obligations towards EU holders.

Overall, an equivalence regime may have merit as a complementary and exceptional access mechanism, provided that it ensures genuinely comparable outcomes and effective enforcement. It should not replace MiCAR authorisation or facilitate regulatory arbitrage. Where equivalent and enforceable safeguards cannot be demonstrated, the relevant global stablecoin should not benefit from facilitated access to the EU market.

Question 41. Equivalence regimes can rely on the third country's regime to various degrees.

How far, in your opinion, should a possible equivalence regime go in terms of relying on third-country regime?

What rights or benefits should EU issuers derive from equivalence of a third country and what rights or benefits in the EU should issuers from an equivalent jurisdiction receive in the EU?

The FMA considers that, should the European Commission decide to permit third-country multi-issuer stablecoin arrangements, an equivalence framework similar to that adopted under the US GENIUS Act could provide a viable approach.

Such a framework could reduce legal uncertainty and facilitate supervisory cooperation while avoiding the need for a full and separate EU authorisation process for each participating issuer. However, participation should be conditional on the relevant third-country framework providing substantially equivalent prudential, supervisory and investor protection outcomes.

In particular, any future equivalence regime should ensure:

- that reserve assets backing EU-related issuance are held within the EU or with appropriately supervised EU entities;
- effective access for EU competent authorities to all supervisory, prudential and reserve-related information necessary for ongoing supervision;
- equivalent AML/CFT and KYC requirements;
- the ability of issuers and competent authorities to freeze, restrict or burn tokens where required by law or supervisory action;
- effective supervisory cooperation and information-sharing arrangements between EU and third-country authorities.

The FMA considers these elements to be essential safeguards for any equivalence-based framework.

At the same time, any future regime should also clarify the treatment of stablecoin arrangements involving jurisdictions that have not been recognised as equivalent. In the absence of equivalence, participation in multi-issuer arrangements should either be prohibited or subject to significantly enhanced

prudential safeguards.

The FMA therefore considers that an equivalence-based approach may offer a more proportionate and operational solution than full localisation requirements, provided that robust safeguards regarding reserves, supervisory access, financial crime prevention and enforcement powers are maintained.

Question 42. What administrative simplification or burden reduction measures should be considered under titles III and IV and their implementing measures and technical standards?

Do you believe that MiCA level 1 provisions lay down proportionate rules for issuers of EMTs and ARTs?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree effective)	5 (strongly agree)	Don't know - No opinion - Not applicable
Authorisation of ARTs and EMTs issuers	☐	☐	☐	☒	☐	☐
Prudential requirements	☐	☐	☐	☒	☐	☐
Governance arrangements	☐	☐	☐	☒	☐	☐
Obligations in respect of specific crypto-asset services	☐	☐	☒	☐	☐	☐

Please explain your answers to question 42:

Question 43. Do you believe that below specified MiCA level 2 acts lay down proportionate and simple-to-apply rules for ART and EMT issuers, taking into account their different size, scope of activity and risk profile?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree effective)	5 (strongly agree)	Don't know - No opinion - Not applicable
RTS on complaint handling by issuers of ARTs (Article 31(5))	☐	☐	☒	☐	☐	☐
RTS on the minimum content of governance remuneration (Article 45(7) (a))	☐	☐	☐	☒	☐	☐

RTS on the information to be submitted in an application for authorisation to issue ARTs (Article 18(6))	☐	☐	☐	☒	☐	☐
COM Delegated Act on ART /EMT significance criteria (Article 43 (11))	☐	☒	☐	☐	☐	☐
RTS on own funds for issuers of ARTs and EMTs (Article 35(6))	☐	☐	☐	☒	☐	☐
an application for authorisation to issue ARTs (Article 18(6))	☐	☐	☐	☒	☐	☐
COM Delegated Act on ART/EMT significance criteria (Article 43 (11))	☐	☒	☐	☐	☐	☐
RTS on own funds for issuers of ARTs and EMTs (Article 35(6))	☐	☐	☐	☒	☐	☐

Please motivate your answers to question 43 and briefly explain what the problems are for your highest-rated issue(s) and suggest how they should be addressed (e.g. legislative clarification, supervisory guidance, industry standards):

The FMA broadly considers the RTS and delegated acts adopted under MiCA to be appropriately calibrated and generally fit for purpose.

In particular, the prudential framework for own funds requirements appears proportionate and well-calibrated given the current state of market development and supervisory experience. The FMA does not currently see evidence that would justify a fundamental revision of the own funds framework or the introduction of substantially more complex methodologies.

The RTS on information to be submitted in an application for authorisation to issue ARTs are comprehensive and, in certain areas, may be regarded as relatively burdensome for applicants. However, given the novelty of the business models and the potential prudential, operational and consumer protection risks involved, the FMA considers the information requirements to be broadly justified and appropriate for supervisory assessment purposes.

Regarding the significance framework, the FMA notes that practical challenges may arise in relation to certain criteria, particularly where reliable and consistent data are difficult to obtain. This may notably be the case for elements such as financial interconnectedness and certain cross-border metrics, where measurement may depend on information that is not always readily available or fully observable by issuers and supervisors.

Nevertheless, the FMA considers the overall significance framework to be appropriate and does not currently see a need for major recalibration. Future refinements should primarily focus on improving the availability, consistency and operability of the underlying data rather than fundamentally changing the existing criteria. Overall, the FMA considers that the MiCA Level 2 framework strikes an appropriate balance between prudential robustness, proportionality and supervisory effectiveness. Further reassessment may be warranted once additional practical experience has been gained, particularly with authorised ART issuers and more complex stablecoin business models.

Question 44. Do issuers identify any need to further standardise reporting requirements for issuers/information flow between CASPs and issuers

for the purposes of MiCA?

☐ Yes

☐ No

☐ Don't know / no opinion / not applicable

Please explain your answer to question 44:

--

PART 3. The appropriateness of the legal framework for crypto-asset service providers (CASPs)

MiCA created a legal framework for crypto-asset service providers. While provisions governing crypto asset service providers have been in operation only since the end of 2024 and a transitional period for service providers that were already on the market is still in place in a number of Member States, a substantial number of crypto asset service providers have now been authorised across a range of Member States and service categories (currently, there are around 170 CASPs listed in the ESMA register – including both authorised CASPs and other entities that have notified to their national competent authorities their intention to provide crypto-asset services. These authorisations or notifications come from 18 different Member States).

This section accordingly seeks stakeholders' feedback on the adequacy of the current scope of crypto-asset services regulated under MiCA and seeks views on the merits of simplification of the framework, any risks not properly accounted for and on the functioning of certain CASP business models in light of MiCA.

3.1 Crypto-asset services

Question 45. Is the list of crypto-asset services as defined in Article 3(16) of MiCA adequate to effectively cover crypto-asset markets and provide sufficient legal clarity for businesses?

- ☐ Yes
- ☒ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 45:

The list of crypto-asset services set out in Article 3(1), point (16), MiCA broadly captures the core intermediation activities currently performed in crypto-asset markets. However, it does not fully reflect all economically relevant services and business models offered by crypto-asset service providers. This creates legal uncertainty where an activity is only partially covered by MiCA or is provided in combination with one or more regulated crypto-asset services.

One relevant example is staking-as-a-service. MiCA does not regulate staking as a separate crypto-asset service. Where a service provider holds clients' crypto-assets or the private keys giving access to them, staking services are currently treated as ancillary to the custody and administration of crypto-assets. While this subjects the provider to the requirements applicable to custody, those requirements do not specifically address all risks associated with staking. These include slashing, lock-up and unbonding periods, delegation to third-party validators, the availability of clients' assets, the calculation and distribution of rewards, and the treatment of losses or penalties.

Crypto-asset lending and borrowing raise similar concerns. These activities constitute an important product line for a number of CASPs but are not included as separate crypto-asset services under MiCA. Where lending or borrowing is offered together with custody, execution or another regulated service, only parts of the overall product may fall within the MiCA framework. This may lead to uncertainty concerning the applicable regulatory requirements and may create the misleading impression that the entire product is subject to MiCA safeguards. Lending and borrowing also entail specific counterparty, credit, liquidity, collateral, concentration and consumer-protection risks that are not adequately addressed through the requirements applicable to related crypto-

asset services.

Furthermore, dealing on own account is not included as a separate crypto-asset service, although it constitutes a regulated investment activity under MiFID II. MiCA covers the exchange of crypto-assets for funds or other crypto-assets, which may involve the use of proprietary capital, but does not provide a distinct framework for CASPs engaging in material proprietary trading outside or alongside such client-facing exchange services. As a result, relevant market, inventory, concentration and conflict-of-interest risks may not be sufficiently captured. The regulatory treatment of own-account dealing should therefore be clarified, including the circumstances in which such activity should trigger additional prudential, organisational, risk-management and conflict-of-interest requirements.

Further uncertainty may arise in relation to hybrid business models, including crypto-asset “earn” products, margin-financing arrangements, prime-brokerage-like services and services facilitating access to DeFi protocols. In such cases, the combination of regulated and unregulated components makes it difficult for both competent authorities and market participants to determine the precise scope of the authorisation and the safeguards applicable to the overall product.

Article 3(1), point (16), should therefore be reviewed and, where appropriate, complemented by additional function-based service categories. In particular, staking-as-a-service and crypto-asset lending and borrowing should be considered for explicit inclusion, subject to proportionate requirements addressing their specific risks. The treatment of dealing on own account should also be clarified.

At the same time, the framework should avoid creating a separate authorisation category for every technical feature or merely ancillary activity. The approach should remain technology-neutral and focus on the economic function of the service, the degree of control exercised over clients’ assets and the risks created for clients and the market. Clear criteria should determine when an activity is merely ancillary to an existing crypto-asset service and when its nature, scale or risk profile requires a separate authorisation or additional safeguards.

Question 46. If additional services should be added, what should those be and what requirements should be applied to these services and service providers?

If you believe that certain services should be removed, please specify which ones and why:

The list of crypto-asset services under MiCAR should be expanded where activities are functionally comparable to regulated financial services or create material risks for clients and markets. In particular, consideration should be given to including crypto-asset lending and borrowing and staking services provided on behalf of clients. These activities are increasingly offered by centralised service providers but are not comprehensively covered by the current MiCAR service catalogue.

For crypto-asset lending and borrowing, the applicable requirements should address, in particular:

- authorisation and organisational requirements;
- clear contractual allocation of rights and obligations;
- disclosure of counterparty, credit, liquidity and collateral risks;
- segregation and safeguarding of client crypto-assets;
- collateral valuation, margining and liquidation procedures;
- concentration and liquidity risk management;

- restrictions on the reuse of client assets without explicit and informed consent;
- prudential safeguards proportionate to the provider's risk exposure; and
- orderly termination, recovery and return of client assets.

The regulatory treatment should distinguish between providers acting merely as intermediaries and providers using their own balance sheet, assuming credit risk or pooling client assets. Requirements should be calibrated accordingly and should avoid overlaps with existing banking, investment services or consumer credit legislation.

Staking services provided on behalf of clients should also be expressly regulated where the provider exercises control over clients' crypto-assets, selects validators, pools assets or distributes staking rewards. Requirements should cover custody and segregation, disclosure of lock-up periods, unbonding arrangements, slashing risks, fees and the calculation of rewards. Providers should also establish appropriate risk-management, business-continuity and validator-selection procedures. Clients should be informed whether the provider guarantees any return or merely passes on protocol-generated rewards. The rules should distinguish custodial staking services from purely technical or non-custodial participation in a decentralised network.

The inclusion of additional services should be based on the substance of the activity rather than terminology used by providers. This would reduce opportunities for regulatory arbitrage and ensure that economically equivalent services are treated consistently. At the same time, activities that are genuinely decentralised and performed without an identifiable intermediary or service provider cannot readily be subjected to conventional authorisation requirements. The existence of decentralised technology should, however, not exempt an identifiable entity that controls the service, determines its essential parameters or maintains an ongoing relationship with clients.

Where services such as staking, lending or borrowing are brought within the regulatory perimeter, appropriate transitional measures should be provided for existing business models, allowing sufficient time for authorisation and operational adjustments while avoiding unnecessary disruption to viable businesses and ensuring timely protection of clients.

At this stage, we do not see a compelling case for removing any of the existing crypto-asset services from MiCAR. Removing services could create supervisory gaps and encourage providers to restructure activities primarily to avoid regulation. Instead, further clarification may be needed regarding the boundaries between certain services, particularly custody, execution of orders, exchange services, transfer services and advice, as business models may combine several functions. Any adjustment should therefore focus on clearer definitions and consistent application rather than narrowing the existing scope.

Question 47. Would the introduction of appropriateness test for the crypto-asset services of reception and transmission, execution and placing of crypto-assets increase the protection for CASP clients, especially retail clients?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 47:

The introduction of an appropriateness assessment for the reception and transmission of orders, execution of orders on behalf of clients and placing of crypto-assets would enhance client protection, particularly for retail clients.

The conduct-of-business framework for CASPs under Title V MiCAR is, in many respects, modelled on the framework applicable to investment firms under MiFID II. However, certain investor-protection mechanisms established under MiFID II were not incorporated into MiCAR. In particular, MiCAR does not require CASPs providing non-advised transaction services to assess whether clients have the necessary knowledge and experience to understand the risks associated with the relevant crypto-asset or service. By contrast, MiFID II requires an appropriateness assessment for non-advised investment services, subject to limited conditions under which services may be provided on an execution-only basis.

This difference is difficult to justify from an investor-protection perspective. Crypto-assets may involve substantial complexity and risks, including high price volatility, liquidity risks, technological and operational risks, loss of private keys, cybersecurity risks, uncertain valuation, complex tokenomics and limited or conditional rights attached to the crypto-asset. Retail clients may not adequately understand these characteristics merely on the basis of general risk disclosures.

An appropriateness assessment would enable CASPs to determine whether a client possesses sufficient knowledge and experience to understand the relevant risks. Where the CASP concludes that the crypto-asset or service is not appropriate, or where the client does not provide sufficient information, the CASP should be required to issue a clear and prominent warning. The framework should also contain requirements concerning the information to be collected, the assessment of clients' knowledge and experience, the classification of crypto-assets according to their complexity, the effectiveness of warnings, record-keeping and periodic review of the assessment methodology.

Any such regime should be proportionate and aligned, as far as appropriate, with Article 25 MiFID II and the corresponding ESMA guidance. Under MiFID II, the appropriateness assessment is an important investor-protection mechanism for non-advised services. It requires firms to obtain information regarding a client's knowledge and experience and to issue a warning where the envisaged product or service is considered inappropriate. This alignment would also reduce unnecessary regulatory divergences where the same provider offers both financial instruments and crypto-assets or where products with comparable economic characteristics fall under different regulatory regimes.

At the same time, the introduction of an appropriateness assessment would require MiCAR to distinguish more clearly between retail and non-retail clients. MiCAR currently does not contain a comprehensive client-classification framework comparable to the distinction under MiFID II between retail clients, professional clients and eligible counterparties. A harmonised definition of retail and non-retail clients would therefore be necessary to ensure consistent application throughout the Union.

The highest level of protection should apply to retail clients. Professional clients or other sufficiently sophisticated clients could be subject to a proportionate regime, including presumptions regarding their knowledge and experience. Any criteria for classification or optional treatment as a professional client should, however, be harmonised at Union level and should not rely solely on self-certification by the client.

Consideration could also be given to a narrowly defined execution-only exemption for non-complex crypto-assets. Such an exemption should apply only where the service is provided at the client's initiative, the crypto-asset meets harmonised criteria for being classified as non-complex, the client is clearly informed that no appropriateness assessment is being performed, and the CASP complies with the applicable conflict-of-interest requirements. Given the particular risks and evolving nature of crypto-assets, the category of non-complex crypto-assets should be interpreted restrictively.

MiCA already requires a suitability assessment for advice on crypto-assets and portfolio management under Article 81. Extending the framework through an appropriateness assessment for non-advised transaction services would therefore complement the existing approach and establish a more coherent, risk-sensitive system of client protection. It would close a material gap in Title V MiCAR without preventing retail clients from accessing crypto-asset markets. The purpose should not be to prohibit transactions considered inappropriate, but to ensure that clients receive an effective warning and are able to make a more informed decision.

Question 48. The provision in the EU of crypto asset services covered by MiCA requires that the service provider is authorised under MiCA and complies with its requirements.

Do you have evidence of non-EU authorised crypto asset services providers continuing to offer their services in the EU?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Question 48.1. How do they promote their services in the EU?

What tools would supervisors or enforcement authorities have, or should they have, to stop non-authorised service providers from offering their services in the EU or to EU customers?

- Key indicators that a market participant is unlawfully targeting the Austrian market with crypto-asset services and is therefore acting in breach of the reverse solicitation principle include, in particular, the design and content of the respective undertaking's website (for example, content available on the website that has a direct connection to Austria) as well as other marketing activities targeting the Austrian market, such as the use of influencer/affiliates or referral programmes. Against this background, it is essential that the reverse solicitation principle and the related guidelines are interpreted and applied consistently across the European Union in order to ensure the effective and harmonised enforcement against unauthorised business activities throughout the EU.
- Enforcement tools currently available in Austria to address unauthorised business are procedural orders, prohibition decisions, administrative penalty proceedings, and as a last resort, website blocking measures. In order to combat the unauthorised provision of crypto-asset services even more effectively in the future, it would be necessary for NCAs across the EU to have the possibility to publish investor warnings (f.e. on their respective websites) where there is already a mere suspicion that such unauthorised activities are being carried out.

Please explain your answer to question 48, specifying what in your view could be a relevant alternative:

3.2 Prudential requirements for CASPs

Article 67 of MiCA provides that prudential safeguards for crypto-asset service providers shall be equal to an amount or at least the higher of an amount of permanent minimum capital or one quarter of fixed overheads of the preceding year, reviewed annually.

Question 49. Is the prudential regime for crypto-asset service providers appropriate to capture the risks associated with the provision of crypto-asset services, or would it be warranted to adjust the prudential stance, e.g. by aligning it with the requirements for own funds applicable to investment firms (including K-factors) that provide services that are broadly similar?

- ☐ It is appropriate to capture the risks associated with the provision of crypto-asset services
- ☒ It would be warranted to adjust the prudential stance
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 49:

The prudential safeguards under Article 67 MiCAR provide a clear and proportionate baseline. However, the current approach, based on permanent minimum capital or one quarter of fixed overheads, does not necessarily reflect the scale and nature of the risks generated by a CASP's activities. In particular, fixed overheads may bear little relation to the volume of client crypto-assets or funds safeguarded, trading activity, client orders handled, or exposures arising from operational, custody and concentration risks. Article 67 MiCAR currently requires safeguards equal to the higher of the applicable permanent minimum capital requirement or one quarter of the preceding year's fixed overheads and allows these safeguards to consist of own funds, insurance or a comparable guarantee.

A more risk-sensitive approach would therefore be warranted, particularly for larger or more complex CASPs and for services involving custody, operation of a trading platform or execution of client orders. Relevant indicators could include, for example, the value of client crypto-assets and client funds safeguarded, trading volumes, client orders handled, balance-sheet exposures and concentration risks.

The investment firm regime and its K-factors may provide a useful conceptual reference, especially where crypto-asset services are functionally comparable to investment services. However, the investment firm framework should not be transposed mechanically. Certain risks specific to crypto-asset services, including loss of private keys, cyber incidents, failures of distributed ledger technology, operational dependencies on third-party service providers and the high volatility or limited liquidity of certain crypto-assets, may require specifically calibrated risk metrics.

Any adjustment should remain proportionate to the nature, scale and complexity of the CASP's activities. A possible approach would be to retain the existing minimum capital and fixed-overheads requirements as a baseline, supplemented by activity-based risk factors for CASPs exceeding defined thresholds. Smaller and less complex CASPs should not be subject to disproportionate calculation and reporting requirements.

The role of insurance policies and comparable guarantees should also be reviewed. Such instruments may appropriately cover certain professional liability and operational risks, but they do not necessarily provide the same loss-absorption capacity as own funds, particularly in periods of market-wide stress or where coverage exclusions apply. For material or systemic CASPs, an appropriate minimum proportion of the prudential safeguards should therefore consist of own funds.

Overall, a more risk-sensitive prudential regime would better capture the actual risk profile of CASPs. It should build on, rather than fully replace, the

existing Article 67 MiCAR framework and should be specifically calibrated to crypto-asset services instead of merely replicating the investment firm regime.

Question 50. Is the amount of minimum capital provided for each class of CASP listed in Annex IV of MiCA adequate or should it be recalibrated? Please rate each minimal requirement on a scale from 1 to 5, where:

- 1 = Significantly decreased (much lower than current MiCA requirements)
- 2 = Somewhat decreased (moderately lower than current MiCA requirements)
- 3 = Kept roughly as is (current MiCA calibration is broadly appropriate)
- 4 = Somewhat increased (moderately higher than current MiCA requirements)
- 5 = Significantly increased (much higher than current MiCA requirements)

	1 (significantly decreased)	2 (somewhat decreased)	3 (kept roughly as is)	4 (somewhat increased)	5 (significantly increased)	Don't know No opinion Not applicable
Minimum initial capital for Class 1 (EUR 50.000)	☐	☐	☐	☒	☐	☐
Minimum initial capital for Class 2 (EUR 125.000)	☐	☐	☐	☒	☐	☐
Minimum initial capital for Class 3 (EUR 150.000)	☐	☐	☐	☐	☒	☐

Please explain your answers to question 50, indicating, if necessary, how the amount of minimum capital should it be recalibrated:

The minimum capital requirements set out in Annex IV MiCA should be recalibrated upwards. The current amounts appear comparatively low considering the operational, market, custody, settlement, counterparty and business-continuity risks associated with the respective crypto-asset services. This is particularly relevant for CASPs operating trading platforms or holding and controlling clients' crypto-assets.

The calibration should also be assessed against the prudential framework applicable to investment firms carrying out economically comparable activities. Under Article 9 of Directive (EU) 2019/2034, the initial capital requirement for investment firms generally ranges from EUR 75,000 to EUR 750,000, depending on the services provided and the risks involved. In particular, investment firms authorised to deal on own account or underwrite financial instruments or place them on a firm commitment basis are subject to an initial capital requirement of EUR 750,000. Other investment firms are generally subject to an initial capital requirement of EUR 150,000, unless the lower EUR 75,000 category applies.

Although the risks and legal characteristics of crypto-asset services are not identical to those of investment services under MiFID II, the substantial differences in minimum capital are not fully justified by the respective risk profiles. MiCA itself establishes a regulatory framework covering the authorisation, operation, organisation and governance of CASPs, as well as the protection of their clients. The minimum capital requirements should therefore provide a credible financial buffer against the material risks arising from those activities.

For Class 1 CASPs, an increase from the current level of EUR 50,000 would be appropriate. The current requirement may be insufficient to ensure an adequate minimum level of financial resilience, particularly where the CASP has a broad cross-border client base.

For Class 2 CASPs, the minimum capital requirement should also be increased. These CASPs may provide custody and administration of crypto-assets on behalf of clients, exchange services or execution services. Such activities can involve direct control over client assets, operational and cybersecurity risks, settlement risks, conflicts of interest and potentially significant liability exposures. A minimum capital requirement of EUR 125,000 appears low where the CASP holds substantial volumes of client crypto-assets or operates a business model with a high degree of operational or counterparty risk.

The need for recalibration is most pronounced for Class 3 CASPs operating a trading platform for crypto-assets. A minimum initial capital requirement of EUR 150,000 does not adequately reflect the potential scale and complexity of such platforms. Trading-platform operators may constitute important market infrastructures and face material operational, technological, market-integrity, liquidity, conflict-of-interest and business-continuity risks. Disruptions or failures may affect a large number of clients and may have broader effects on market functioning. The current difference between the Class 2 and Class 3 requirements is also too limited to reflect the additional risks associated with operating a trading platform.

A further relevant consideration is that CASPs are not generally covered by a harmonised investor-compensation scheme comparable to the protection available in the investment-services sector. Consequently, clients may bear losses directly where a CASP is unable to return assets or meet liabilities and the applicable liability, segregation or insolvency safeguards prove insufficient. Higher minimum capital cannot replace an investor-compensation scheme, but it can strengthen the CASP's loss-absorbing capacity and reduce the probability that operational incidents, liability claims or business failures result in uncompensated client losses.

Recalibration should nevertheless remain proportionate and should not rely exclusively on substantially increasing the fixed amounts in Annex IV. The permanent minimum capital should function as a credible entry threshold and backstop. It should be complemented by more risk-sensitive ongoing own-funds requirements reflecting, where relevant, the volume of client assets safeguarded or controlled, trading and transaction volumes, operational expenditure, proprietary positions, counterparty exposures and the scale and complexity of the CASP's activities.

The recalibrated framework could therefore combine higher permanent minimum capital requirements, particularly for Class 3 CASPs, with activity-based or exposure-based components. This would achieve greater consistency with the prudential logic applicable to investment firms while recognising the specific characteristics of crypto-asset services and avoiding disproportionate burdens on small CASPs with genuinely limited risk profiles.

3.3 Multi-function groups

MiCA recognises and supports multi-function groups in which issuers, crypto-asset service providers (CASPs) may provide multiple MiCA-scope crypto-asset services, or may also carry out other types of financial activity, based on proper governance and management of the conflicts of interest this may generate.

Question 51. Should the current approach be maintained or should there be enhanced oversight and coordination in relation to entities that in addition to providing crypto-asset services, offer (1) other unregulated services or (2) other types of regulated services, (3) a combination of crypto-asset services? What kind of action would be appropriate?

- ☐ The existing approach should be maintained
- ☒ There should be enhanced oversight and coordination in relation to such entities
- ☐ Don't know / no opinion / not applicable

Question 51.1. Which of the following enhanced oversight and coordination mechanisms do you consider may be appropriate?

Please select as many answers as you like

- ☒ Group-level reporting to a centralised authority
- ☒ Enhanced supervisory cooperation between ESAs / NCAs
- ☒ Operation of new supervisory colleges
- ☒ Consolidated supervision
- ☒ Other

Please specify to what other mechanism(s) you refer in your answer to question 51.1:

Where several licensed entities of the same group, such as a CASP, investment firm, payment institution or electronic money institution, are established in the same Member State, the relevant NCA or NCAs should exercise coordinated oversight. This enables a more comprehensive assessment of the group's governance, intra-group dependencies, conflicts of interest, outsourcing arrangements and risks across different regulated activities.

The supervisory assessment should not be limited to separately authorised entities. Multi-function groups frequently combine regulated financial and crypto-asset services with activities that are not regulated, or are only partially regulated, under MiCAR or other EU financial-services legislation. Examples include staking, crypto-asset lending and borrowing, proprietary trading, technology services and access to DeFi protocols. Such activities may create material risks for regulated entities and their clients.

Competent authorities should therefore be able to assess unregulated group activities insofar as they may affect a regulated entity. Relevant risks include intra-group exposures, shared infrastructure and clients, common liquidity sources, transfers or reuse of client assets, centralised treasury functions, operational dependencies and contagion risks. This would not amount to treating all unregulated group activities as regulated. However, regulated entities should provide sufficient group-level information and demonstrate that risks originating elsewhere in the group are appropriately identified, managed and insulated from the regulated entity.

This is particularly important where the group uses common branding or an integrated digital interface. Clients may not understand which group entity provides a service, whether the service is regulated and which protections apply. Regulated and unregulated services should therefore be clearly distinguished, responsibilities transparently allocated and conflicts of interest effectively managed.

Where relevant group entities are established in several Member States, a lead authority should be designated on the basis of harmonised criteria. These should include the location of the group's main EU decision-making functions, the relative importance of its regulated entities, the volume of EU business, the number of clients and the location of material risks and critical functions. The designation should reflect the group's actual operational structure rather than solely its formal legal structure.

The lead authority should receive consolidated group-level reporting and coordinate the assessment of cross-entity and cross-border risks. Such reporting should cover regulated and unregulated activities, intra-group exposures, concentration risks, shared infrastructure, outsourcing, governance, conflicts of interest and dependencies on third-country entities. Entity-level supervision and formal supervisory powers should remain with the respective home NCA.

Supervisory colleges should be established for relevant cross-border groups, particularly where the group contains several sectorally regulated entities, relies on shared critical functions or provides services on a significant scale in several Member States. Colleges should facilitate information exchange and coordinate risk assessments, supervisory measures and crisis management.

The ESAs should foster cross-sectoral supervisory cooperation and convergence at EU level. This should include common criteria for identifying relevant groups, harmonised group-reporting requirements, effective information-sharing arrangements and consistent standards for supervisory colleges. The ESAs should also support coordination and, where necessary, mediation between the competent authorities involved.

Please explain your answer to question 51.1. and provide any comments on the operational feasibility, legal implications, proportionality, or potential unintended consequences of the measures above:

Enhanced oversight is warranted because entity-by-entity supervision may not provide a complete view of risks arising within multi-function groups. Such groups may combine several crypto-asset services, regulated financial services and unregulated activities across different entities and jurisdictions. This can create material intra-group dependencies, conflicts of interest, contagion risks, regulatory arbitrage and uncertainty regarding the allocation of responsibilities and the location of client assets.

However, the proposed mechanisms should not apply automatically or cumulatively to every group containing a CASP. Their application should be proportionate and based on harmonised criteria such as the group's size, complexity, cross-border activity, range of regulated and unregulated services, volume of client assets, intra-group exposures, outsourcing intensity and reliance on shared ICT or operational infrastructure.

Group-level reporting would be operationally feasible and useful if based on standardised and proportionate templates. It should cover the group's legal and organisational structure, regulated and unregulated activities, intra-group exposures and asset flows, shared infrastructure, critical outsourcing, concentration risks and material conflicts of interest. Reporting should focus on information not already available through entity-level reporting and should follow a "report once" principle. The receiving authority should be able to share relevant information with other competent authorities while respecting confidentiality and data-protection requirements.

Enhanced cooperation between ESAs and NCAs should be the primary mechanism for groups subject to several EU regulatory frameworks or operating across multiple Member States. Cooperation should include regular information exchange, coordinated risk assessments, allocation of supervisory responsibilities and procedures for material incidents and crisis situations. It should also address cooperation with third-country authorities where material group entities or functions are located outside the EU.

Supervisory colleges could be appropriate for large, complex or materially cross-border groups where bilateral cooperation is insufficient. They should not be mandatory for smaller or less interconnected groups. Existing colleges under other sectoral legislation should be used or expanded where practicable to avoid parallel structures, overlapping requests and inconsistent supervisory expectations. MiCAR colleges currently relate primarily to issuers of significant ARTs and EMTs and do not provide a general framework for CASP-led multi-function groups.

Consolidated supervision should be reserved for groups whose aggregate activities, intra-group exposures or shared infrastructure create material risks that cannot be adequately assessed at entity level. Its scope should be clearly defined and could include group-wide governance, risk management, conflicts of interest, concentration, prudential risks, outsourcing and recovery planning. Consolidation should not automatically extend MiCAR requirements to all unregulated group entities. Rather, competent authorities should have access to information necessary to assess risks posed by those entities to the regulated CASP and its clients.

As an additional mechanism, a group coordinator or lead supervisory authority should be designated for qualifying groups. The coordinator should maintain a group-wide risk assessment, coordinate supervisory planning and facilitate joint action where necessary. The designation should follow objective criteria and should not override the statutory responsibilities of sectoral or national competent authorities.

Potential unintended consequences include duplicative reporting, multiple authorities requesting the same information, conflicting supervisory measures, excessive burdens for smaller groups and uncertainty regarding the division of responsibilities. Clear rules are therefore needed on thresholds, scope, information sharing, decision-making and the relationship between group-level and entity-level supervision.

Enhanced coordination must not dilute the responsibility of the individual authorised CASP. Each CASP should retain sufficient substance, management capacity, expertise, access to information and operational control to comply with MiCAR, even where important functions are performed by other group entities. Group-level oversight should supplement, rather than replace, the accountability and effective supervision of each regulated entity.

Please explain your answer to question 51:

Multi-function groups can generate risks that are not adequately captured through entity-by-entity supervision. These risks may arise where CASPs combine several crypto-asset services, provide regulated and unregulated services within the same entity or group, or form part of a wider financial or non-financial group.

Relevant risks include conflicts of interest, intra-group dependencies and exposures, concentration of critical functions, contagion, regulatory arbitrage and

the transfer of risks or activities between regulated and unregulated group entities. Complex legal and operational structures may also make it difficult to identify where client assets are held, which entity performs a particular function and which entity is responsible towards clients. These concerns are particularly relevant for groups operating across several Member States or involving material third-country entities.

Enhanced oversight should not prohibit multi-function business models. Combining services may create operational efficiencies and allow clients to access several services through a single regulated provider. However, competent authorities need a sufficiently comprehensive view of the group's structure, activities, dependencies and aggregate risk profile.

The intensity of enhanced oversight should be proportionate and based on factors such as the group's size, complexity, cross-border activity, volume of client assets, range of services, intra-group exposures, outsourcing dependencies and involvement of unregulated or third-country entities. Enhanced requirements should focus on material risks rather than impose full consolidated supervision on every group containing a CASP.

3.4 Reporting

Apart from the obligation to report any reasonable suspicion regarding an order or transaction where there might exist circumstances indicating that market abuse has been committed, is being committed or is likely to be committed, there are no formal reporting obligations for CASPs in MiCA.

Question 52. Should CASPs report regularly their activities?

	Yes	No	Don't know – No opinion - Not applicable
Direct holdings of crypto-assets by CASPs	☒	☐	☐
Large exposures to derivatives with crypto-assets as the underlying asset	☐	☒	☐
Volumes of leveraged contracts and the extent to which leverage is actually used on trading platforms	☐	☒	☐
Information on counterparty risk	☒	☐	☐

Please specify what kind of reporting would be useful and how often? Please explain:

- Considering consumer and investor protection, regular reporting by CASPs on the points outlined should, in principle, be supported. From a consumer protection perspective, it is crucial that the data collected serve not only for market monitoring but also enable supervisors to identify risks to customers and their assets at an early stage.
- The reporting requirements should be proportionate to and consider the size, complexity, and risk profile of the respective CASP. Regular reporting should be complemented by event-driven notifications covering material changes to the CASP's governance, ownership, organisation and business model. Reporting limited to financial exposures and activity volumes would not provide competent authorities with sufficient information to assess whether the conditions for authorisation continue to be met.

CASPs should submit periodic, standardised information on:

- the type and volume of crypto-asset services provided;
- client numbers and transaction volumes;
- crypto-assets and funds held or safeguarded for clients;
- own-account holdings of crypto-assets and related material exposures;
- prudential safeguards and own funds;
- material counterparty, concentration and liquidity risks;
- complaints and material compliance breaches;
- material outsourcing arrangements; and
- significant operational or security incidents, without duplicating reporting under DORA.

Periodic reporting could generally be required annually, with semi-annual or quarterly reporting for larger, more complex or systemically relevant CASPs. The frequency should be proportionate to the nature, scale and complexity of the activities performed.

More importantly, MiCAR should establish harmonised event-driven notification requirements. CASPs should notify the competent authority without undue delay, and where appropriate in advance, of material changes including:

- the appointment, replacement, prolonged absence or departure of holders of key functions, such as compliance, risk management, internal audit functions;
- material changes to the responsibilities or organisational position of those functions;
- mergers, transformations, divisions, capital measures, dissolution or other material corporate actions;
- material changes to the business model, services provided or geographical scope;
- the establishment or closure of branches;
- material outsourcing arrangements or changes thereto; and
- circumstances materially affecting the suitability of management body members, qualifying shareholders or key function holders.

To ensure consistent supervision, MiCAR should define relevant key functions, taking into account the nature, scale and complexity of the CASP. Common EU templates, materiality thresholds and notification deadlines should be introduced. Critical changes should be reported immediately or in advance, while less significant changes could be included in periodic reporting.

The reporting framework should be risk-based and proportionate and should avoid duplicating information already reported under MiFID II, DORA, AML/CFT legislation or other Union law. Competent authorities should be able to request more frequent or granular reporting where justified by the CASP's risk profile.

Please explain your answer to question 52:

CASPs should be subject to regular reporting requirements. However, the categories proposed in the consultation do not yet constitute a coherent reporting framework, as they combine different types of risk and partly relate to activities or instruments that may fall outside the scope of MiCA. Any future reporting regime should therefore be risk-based, harmonised and proportionate, and should primarily relate to the crypto-asset services provided under MiCA.

Information on CASPs' direct holdings of crypto-assets may be relevant for assessing proprietary trading, market, concentration and liquidity risks. Such reporting would only be meaningful, however, if it clearly distinguished the CASP's own holdings from crypto-assets held in custody on behalf of clients. It should also include information on the type, amount, purpose and concentration of the CASP's own holdings, as well as the extent to which those holdings are used for liquidity provision, treasury purposes, client transactions or other activities.

Large exposures to derivatives with crypto-assets as the underlying asset may provide relevant information on concentration, counterparty and contagion risks. However, crypto-asset derivatives generally qualify as financial instruments and are therefore subject to MiFID II, EMIR and other relevant sectoral frameworks rather than MiCA. Introducing a separate MiCA reporting obligation for the same exposures could result in duplicative reporting and unclear supervisory responsibilities. Such information should therefore primarily be collected under the applicable sectoral legislation and made available to the competent MiCA authority through effective information-sharing arrangements where necessary.

The same considerations apply to reporting on the volumes of leveraged contracts and the actual use of leverage on trading platforms. This information

could be relevant for monitoring leverage, forced liquidations, liquidity risks and the amplification of market movements. However, it must first be determined whether the relevant products and activities fall within the scope of MiCA. A reporting requirement based solely on aggregate volumes would also provide limited supervisory value unless it were supplemented by information on actual exposures, collateralisation, leverage ratios, liquidation mechanisms and the composition of the relevant client base. These data should not be collected under MiCA where they are already reported under MiFID II, EMIR or another Union framework.

Information on counterparty risk may be relevant, particularly where CASPs have material exposures to liquidity providers, custodians, settlement counterparties, affiliated entities or other service providers. However, the proposed category is currently too broad and insufficiently defined. Any reporting obligation should be limited to material exposures and should be based on harmonised thresholds, exposure-calculation methods and counterparty categories. Intra-group exposures and concentration risks should be separately identifiable where they are material.

More generally, a MiCA reporting framework should focus on information directly relevant to the services and risks of CASPs. This could include the volume and concentration of client crypto-assets held in custody, client funds, trading and transfer volumes, complaints, material outsourcing arrangements, operational and security incidents, own holdings of crypto-assets, liquidity risks and material counterparty exposures. The scope and frequency of reporting should reflect the nature, scale and complexity of the CASP's activities. More frequent reporting may be justified for large or systemically relevant CASPs, whereas less complex CASPs should be subject to proportionate requirements.

To avoid unnecessary administrative burdens, a "report once" principle should apply. Information already reported under MiFID II, EMIR, DORA or other Union legislation should not be collected again under MiCA. Instead, the relevant authorities should be able to exchange and reuse existing supervisory data. Reporting templates, definitions, calculation methods, materiality thresholds and reporting frequencies should be harmonised at Union level to ensure comparability and consistent supervision across Member States.

3.5 Environmental and sustainability reporting

MiCA strengthens transparency on the environmental impact of crypto-assets. It does so by

- requiring white papers to contain information on the main adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism used to issue the crypto-asset
- requiring CASPs to make that information prominently available for each crypto-asset where they provide services

Question 53. Based on your experience to date, how do you assess the current environmental/sustainability disclosure regime under MiCA (including the relevant Level 2 RTS)?

- ☐ Fully appropriate and proportionate
- ☐ Broadly appropriate, with limited areas for clarification
- ☐ Partially appropriate, but improvements could be considered
- ☐ Not appropriate
- ☒ Don't know / no opinion / not applicable

Please explain your answer to question 53:

--

3.6 Other issues

Question 54. Given that crypto-asset service providers are entities subject to the regulatory framework of the Digital Operational Resilience Act (DORA), are there any additional issues/challenges that need to be addressed in relation to cybersecurity?

Question 55. The Payment Services Directive has been substantially reviewed recently, bringing notably more clarity on the interplay between the MiCA rules applying to the transfer services in relation to e-money tokens and the rules under the payment services framework which apply to the provision of payment services. As a result, the PSD3/R will clarify which crypto-asset services may qualify as payment services, including targeted exclusions from the scope of PSD3/R for specific types of transactions/exchanges involving EMTs, and will specify the authorisation process under PSD3 in cases where CASPs are required to obtain a PSD3 authorisation.

Do you consider these changes bring sufficient clarity or are there other issues that remain to be addressed?

- ☐ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 55:

Question 56. Do MiCA provisions governing crypto asset service providers sufficiently allow, or unduly restrict, access for EU consumers and investors to non-EU and global crypto asset trading and liquidity pools?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 56:

MiCAR strikes an appropriate balance between protecting the EU regulatory perimeter and preserving the freedom of EU consumers and investors to access third-country crypto-asset services at their own initiative.

Article 61 MiCAR provides for reverse solicitation for good reason. Where an EU client, acting independently and without prior solicitation, decides to approach a third-country CASP, the principle of contractual freedom supports allowing that client to access the requested service. A general prohibition on EU clients accessing non-EU trading venues or global liquidity pools would be disproportionate and difficult to reconcile with this principle.

At the same time, reverse solicitation must remain a narrowly construed exception and must not become an alternative route for third-country CASPs to access the EU market without authorisation. Article 61 MiCAR therefore correctly requires that the provision of the service be initiated at the client's own exclusive initiative. Solicitation, promotion or advertising by the third-country CASP, by an entity acting on its behalf or by a closely linked entity precludes reliance on this exemption. ESMA's guidelines appropriately support a restrictive and fact-based application of this concept.

In particular, third-country CASPs should not be able to circumvent MiCAR through targeted online advertising, influencers or affiliates, EU-specific promotional campaigns, localised websites or applications, search-engine optimisation directed at EU users, or contractual disclaimers that merely state that the relationship was initiated by the client. The assessment should be based on the actual conduct of the third-country CASP and all relevant circumstances, rather than on contractual declarations alone.

Effective enforcement is therefore essential. Competent authorities should have adequate powers and tools to identify unlawful solicitation, including in digital channels, and to take action against third-country CASPs that actively target EU clients without authorisation. Cooperation between national competent authorities and ESMA should ensure consistent application across the Union and prevent circumvention through differences in national supervisory practices.

Overall, the current approach under MiCAR sufficiently allows access to non-EU and global trading and liquidity pools where this reflects the genuine and exclusive initiative of the EU client. It does not unduly restrict contractual freedom. However, preserving this access requires strict enforcement to ensure that third-country CASPs cannot actively target the EU market or use reverse solicitation as a systematic business model without complying with MiCAR.

Question 56.1 What are the advantages and disadvantages of focusing on EU liquidity or full access to global liquidity?

Focusing exclusively or predominantly on EU liquidity would not be a viable approach. Crypto-asset markets are inherently global, operate continuously across jurisdictions and depend on globally integrated trading venues, market makers and liquidity providers. The EU market currently does not offer sufficient liquidity across all relevant crypto-assets and trading pairs to support competitive execution conditions on a stand-alone basis.

An EU-only approach would therefore be likely to result in shallower order books, wider bid-ask spreads, increased price volatility and less efficient price formation. It could also reduce the availability of crypto-assets and trading pairs for EU clients and adversely affect the ability of CASPs authorised under MiCAR to achieve competitive execution outcomes. Fragmentation of trading and settlement infrastructures generally divides liquidity and increases integration costs.

Furthermore, the EU cannot effectively isolate itself from global crypto-asset markets. Restricting access to global liquidity would not prevent EU clients from seeking such liquidity. Instead, clients could migrate to non-EU providers, decentralised protocols or other channels outside the EU regulatory perimeter. This would weaken rather than strengthen investor protection, as the relevant activities would no longer be conducted through CASPs authorised and supervised under MiCAR. Such an outcome would also disadvantage compliant EU CASPs without materially reducing the underlying risks for EU clients.

Access to global liquidity is therefore essential for the competitiveness and practical viability of the EU crypto-asset market. It can provide deeper order books, narrower spreads, more reliable price formation and better execution quality. It also allows EU clients to access global markets through CASPs subject to MiCAR rather than through unauthorised third-country providers. From a supervisory and investor-protection perspective, facilitating access to

global liquidity through a fully responsible EU-authorised CASP is preferable to driving clients towards providers outside the EU regulatory framework.

At the same time, access to global liquidity must not be unrestricted or used to circumvent MiCAR. Reliance on non-EU trading venues, liquidity providers or group entities may create counterparty, concentration, legal, operational and data-access risks. Differences in regulatory standards may also increase the risk of regulatory arbitrage and external contagion. These risks should be addressed through targeted safeguards rather than by attempting to confine liquidity to the EU.

CASPs accessing global liquidity should remain fully responsible for compliance with MiCAR, including their conduct-of-business, conflicts-of-interest, outsourcing, custody and execution obligations. They should conduct robust initial and ongoing due diligence on non-EU trading venues, liquidity providers and counterparties. They should also maintain effective concentration limits, contractual protections, contingency arrangements and exit strategies, and ensure access to the order, transaction and counterparty data required for their own controls and for supervision by the competent authority.

In particular, an EU-authorised CASP should not operate merely as a client-facing interface or formal gateway for an unregulated third-country platform. The authorised EU entity must retain sufficient substance, operational control, decision-making capacity and risk-management capabilities. It must be able to monitor and control the execution of client orders and remain accountable towards both its clients and the competent authority.

The appropriate policy objective should therefore not be to focus on EU liquidity at the expense of global liquidity. The objective should be to enable CASPs authorised under MiCAR to access global liquidity under conditions that preserve effective EU supervision, investor protection and market integrity. Measures to develop deeper and more competitive liquidity pools within the EU are desirable, but they should complement rather than replace access to global markets. An attempt to separate the EU from global crypto-asset liquidity would be economically unrealistic, detrimental to execution quality and likely to encourage activity to migrate outside the MiCAR regulatory perimeter.

Question 57. Do you believe that the below specified groups of MiCA level 1 provisions lay down proportionate and simple-to-apply rules for CASPs, taking into account their different size, scope of activity and risk profile?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
Authorisation of crypto-asset service providers	☐	☐	☒	☐	☐	☐
Prudential requirements	☐	☒	☐	☐	☐	☐
Governance arrangements	☐	☒	☐	☐	☐	☐
Obligations in respect of specific crypto-asset services	☐	☒	☐	☐	☐	☐
Other Title V rules	☐	☐	☒	☐	☐	☐

Please explain your ratings in question 57 and suggest how rules could be made simpler and more proportionate (e.g. legislative clarification,

supervisory guidance, industry standards):

MiCAR provides an important harmonised framework for the authorisation and supervision of CASPs. However, its Level 1 provisions do not always adequately reflect differences in the size, business model, organisational structure and risk profile of CASPs. Although proportionality is referenced throughout MiCAR, limited guidance is provided on its practical application, creating legal uncertainty and potentially divergent supervisory approaches.

The authorisation framework under Article 62 MiCAR enables competent authorities to conduct a comprehensive assessment of applicants. However, largely identical requirements apply to CASPs with significantly different activities and risk profiles. A more modular approach should distinguish between information required from all applicants and additional information triggered by factors such as the services provided, custody of client assets, outsourcing arrangements, cross-border activities or other relevant risks. At the same time, proportionality should not affect core requirements relating to governance, management suitability, ICT resilience, safeguarding of client assets or the substance of the authorised EU entity.

The prudential framework is insufficiently risk-sensitive. Current requirements are primarily based on fixed minimum capital and fixed overheads and do not adequately capture risks arising from client assets, transaction volumes, proprietary positions, counterparty exposures or operational complexity. Minimum capital requirements should be increased, particularly for CASPs operating trading platforms, and supplemented by proportionate activity- or exposure-based requirements. This is especially relevant given the absence of a harmonised investor-compensation scheme comparable to that available in the investment services sector.

The governance framework establishes an appropriate baseline but requires further clarification regarding its proportional application. CASPs differ considerably in size, complexity and reliance on outsourcing. MiCAR does not provide sufficiently clear criteria regarding organisational substance, staffing, segregation of functions or the independence of control functions.

Particular concerns arise where authorised CASPs rely extensively on group entities or third-party providers for operational, technical or control functions. In such cases, the authorised entity may formally comply with governance requirements while lacking sufficient personnel, expertise, or technical capabilities to exercise effective control. MiCAR should therefore clarify that proportionality cannot justify insufficient substance within the authorised entity. CASPs should retain adequate local management capacity, expertise, access to information and operational control to meet their obligations and effectively engage with competent authorities.

Additional supervisory guidance should clarify the proportional application of risk management, compliance and internal audit requirements, as well as criteria for assessing control-function independence, management involvement, outsourcing arrangements and the accumulation of functions in smaller firms. Simplification should focus on avoiding unnecessary duplication while maintaining effective oversight and accountability.

The provisions governing specific crypto-asset services are not fully comprehensive. Economically important activities such as staking-as-a-service and crypto-asset lending and borrowing are not regulated as standalone crypto-asset services and may be only partially covered where combined with another regulated activity. MiCAR also lacks a distinct framework for material dealing on own account. This creates uncertainty regarding the regulatory perimeter and the safeguards applicable to products combining regulated and unregulated elements. The list of crypto-asset services should therefore be reviewed on a technology-neutral and function-based basis.

Other Title V provisions provide a reasonable baseline but contain investor-protection and reporting gaps. While the framework is broadly modelled on MiFID

II, certain safeguards have not been replicated. In particular, MiCAR does not require appropriateness assessments for reception and transmission, execution or placing services. Consideration should be given to introducing such assessments together with a harmonised distinction between retail and non-retail clients. MiCAR should also provide for proportionate and harmonised reporting requirements while avoiding duplication with MiFID II, EMIR, DORA and other Union legislation.

Overall, simplification should be achieved through legislative clarification, harmonised supervisory guidance, standardised templates and clear thresholds rather than by weakening substantive requirements. A modular and risk-based approach would improve proportionality, legal certainty and supervisory convergence while preserving effective governance and investor protection throughout the Union.

Question 58. Do you believe that below specified MiCA level 2 acts lay down proportionate and simple-to-apply rules for CASPs, taking into account their different size, scope of activity and risk profile?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion- Not applicable
RTS on complaint handling for CASPs (Article 71(5))	☐	☒	☐	☐	☐	☐
RTS on offering pre-trading and post-trading data to the public (Article 76 (16)(a))	☐	☐	☐	☐	☐	☐
RTS on content and format of order book and records to be maintained (Article 76 (16)(b))	☐	☐	☐	☐	☐	☐
RTS on records to be kept of all crypto-asset services, activities, orders and transactions undertaken (Article 68 (10)(b))	☐	☐	☐	☐	☐	☐
RTS on the continuity and regularity in performance of crypto services (Article 68 (10)(a))	☐	☐	☐	☐	☐	☐

Please explain your ratings in question 58 and suggest how rules could be made simpler and more proportionate:

- In order to ensure a level playing field for all financial market participants, the requirements relating to the handling of complaints should be aligned:
- It should therefore be clarified that the analysis of complaint data should not merely serve to improve the handling of complaints, but should in particular also aim to identify and address recurring or systemic issues and potential legal and operational risks. This should include, in particular, identifying root causes, assessing their potential impact on other processes or products, and addressing such root causes.
- Based on supervisory experience, further clarification would be desirable, in particular regarding the interpretation of “available remedies”. In addition, harmonised categories for complaint topics and investigation outcomes would improve the comparability of complaint data across CASPs.
- Additionally, Article 8 of the RTS on complaint handling should clarify that a complaint cannot be considered handled solely on the basis that it has been forwarded to another department. The complaint management function should monitor the handling of the complaint by the relevant department through to

its final resolution and record the outcome.

- Ultimately, a dedicated provision should be included to ensure procedural fairness and the avoidance of conflicts of interest. Reliance on the recitals alone does not provide a sufficiently clear regulatory framework.

PART 4. Policy areas beyond the current scope of MiCA

The following sections seek feedback from stakeholders on these areas, as well as some additional topical issues that are not currently directly regulated by MiCA.

4.1 Decentralised finance

This section refers to decentralised finance (DeFi), understood as software programs deployed on blockchains or other types of DLT that operate autonomously without intermediaries and offer financial functionalities such as trading, lending, borrowing or portfolio management. In the broader sense, DeFi also refers to any blockchain-based application, including an application that does have an identifiable intermediary or person exercising control over its operation. MiCA excludes from its scope 'crypto-asset services that are provided in a fully decentralised manner without any intermediary (MiCA Recital 22: "Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation"). This section seeks feedback on whether and how to complement MiCA as regards DeFi considering potential opportunities and challenges.

Question 59. In case you are aware or make use of DeFi currently beyond the regulatory perimeter of MiCA, what are the main services you (would) use and for which of them do you consider they bring benefits compared to similar intermediated digital assets services?

a) Exchange services

- ☐ DeFi applications present **limited interest** and are **moderately used** for this service
- ☒ DeFi applications present **important potential benefits** for this service but their **use remains limited** due to some non-mitigated weaknesses
- ☐ DeFi applications present **important benefits** for this service and are **already significantly used**, despite **important non-mitigated weaknesses**
- ☐ DeFi applications present **important benefits** for this service, they are **already significantly used** and **present limited risks**
- ☐ Don't know / no opinion / not applicable

b) Payments and transactions services

- ☒ DeFi applications present **limited interest** and are **moderately used** for this service
- ☐ DeFi applications present **important potential benefits** for this service but their **use remains limited** due to some non-mitigated weaknesses
- ☐ DeFi applications present **important benefits** for this service and are **already significantly used**, despite **important non-mitigated weaknesses**
- ☐ DeFi applications present **important benefits** for this service, they are **already significantly used** and **present limited risks**
- ☐ Don't know / no opinion / not applicable

c) Trading and investment services

- ☐ DeFi applications present **limited interest** and are **moderately used** for this service
- ☒ DeFi applications present **important potential benefits** for this service but their **use remains limited** due to some non-mitigated weaknesses
- ☐ DeFi applications present **important benefits** for this service and are **already significantly used**, despite **important non-mitigated weaknesses**
- ☐ DeFi applications present **important benefits** for this service, they are **already significantly used** and **present limited risks**
- ☐ Don't know / no opinion / not applicable

d) Lending and borrowing services

- ☒ DeFi applications present **limited interest** and are **moderately used** for this service
- ☐ DeFi applications present **important potential benefits** for this service but their **use remains limited** due to some non-mitigated weaknesses
- ☐ DeFi applications present **important benefits** for this service and are **already significantly used**, despite **important non-mitigated weaknesses**
- ☐ DeFi applications present **important benefits** for this service, they are **already significantly used** and **present limited risks**
- ☐ Don't know / no opinion / not applicable

e) Custody services

- ☐ DeFi applications present **limited interest** and are **moderately used** for this service
- ☐ DeFi applications present **important potential benefits** for this service but their **use remains limited** due to some non-mitigated weaknesses
- ☒ DeFi applications present **important benefits** for this service and are **already significantly used**, despite **important non-mitigated weaknesses**
- ☐ DeFi applications present **important benefits** for this service, they are **already significantly used** and **present limited risks**
- ☐ Don't know / no opinion / not applicable

Please detail the benefits or weaknesses you associate with the use of DeFi applications for these different services in question 59, and the actions you would consider appropriate to optimise these benefits or address the possible issues they raise:

The FMA generally agrees that certain DeFi applications may offer potential benefits in specific use cases, particularly regarding automation, programmability and the reduction of certain operational frictions.

At the same time, current market developments suggest that the practical adoption of DeFi remains more limited than often anticipated. A significant portion of activity continues to be concentrated within the crypto-asset ecosystem itself rather than serving the wider real economy or mainstream financial markets.

For exchange, trading and investment-related services, DeFi may offer efficiency gains in certain areas. However, operational, legal and governance risks remain only partially mitigated. User protection, accountability, dispute resolution and compliance with regulatory requirements continue to represent significant challenges.

For payments and transaction services, the FMA currently sees limited evidence of widespread adoption. In the EU, efficient payment infrastructures already exist, including instant payments and established electronic payment solutions. As a result, the additional benefits offered by DeFi-based payment services remain unclear in many cases.

Similarly, lending and borrowing applications continue to face important limitations. Many current DeFi lending models rely on substantial overcollateralisation and remain closely linked to crypto-asset market dynamics. Consequently, their economic function differs significantly from traditional credit intermediation.

The FMA acknowledges that custody-related DeFi solutions are among the more established use cases. However, even in this area, significant challenges remain regarding governance arrangements, operational resilience, recovery of assets and accountability in the event of failures or incidents.

Overall, the FMA considers that DeFi exhibits promising technological features and may continue to evolve in specific niche applications. Nevertheless, actual adoption remains relatively limited and several important legal, operational and prudential weaknesses have not yet been fully addressed. As such, the FMA does not currently consider DeFi services to have achieved broad mainstream adoption within the EU financial system.

Question 60. What do you consider to be the main risks associated with DeFi?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
Operational risk	☐	☐	☒	☐	☐	☐
Money laundering and terrorist financing risk	☐	☐	☐	☐	☒	☐
Market abuse	☐	☐	☐	☒	☐	☐
Investor protection risk (information asymmetry, no redress, opacity of functioning)	☐	☐	☐	☐	☒	☐
Financial stability	☐	☐	☒	☐	☐	☐

Please explain your answers to question 60:

Some risks related to ML/TF will depend on the nature and design of DeFi-applications (DeFi services)

DeFi typically involves significant information asymmetries, limited transparency regarding governance and protocol risks, the absence of regulated intermediaries, and little or no effective redress mechanism for users and authorities. Retail investors may also struggle to understand the technical and financial risks associated with DeFi protocols, increasing the likelihood of consumer detriment.

Question 61. In case you consider the criteria for establishing whether a DeFi application is not fully decentralized not sufficiently clear, which of them should do you consider should be used to assess the degree of decentralisation?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
Existence of an identifiable intermediary (person or group of persons) providing a crypto-asset service	☐	☐	☐	☐	☒	☐
Presence of control by an identifiable person or group of persons (e.g. via admin keys) over the key functionalities of a DeFi protocol (e.g. upgradeability of protocol)	☐	☐	☐	☐	☒	☐
Significant concentration of governance power over the key functionalities of a DeFi protocol	☐	☐	☐	☐	☒	☐
Custody of user assets by the DeFi protocol	☐	☐	☒	☐	☐	☐
DeFi protocol code is not open source	☐	☒	☐	☐	☐	☐
Marketing of a DeFi protocol by an identifiable entity or person	☐	☐	☒	☐	☐	☐
Other	☐	☐	☐	☐	☐	☒

Please specify to what other criteria(s) you refer in your answer to question 61:

E.g. the governance structure in relation to governance tokens; control over the frontend, domain names and other critical infrastructure; the ability to censor transactions, exclude users or freeze assets.

The criteria for determining whether a DeFi application is fully decentralised should be clarified at Level 1 or through harmonised EU guidance. The assessment should be based on substance over form and consider the protocol's entire operational lifecycle. A protocol should not be regarded as fully decentralised merely because transactions are executed automatically through smart contracts or governance is formally assigned to token holders.

The most relevant criterion is whether an identifiable person or coordinated group provides the relevant crypto-asset service or exercises material control over it. This includes the ability to deploy, upgrade, pause or terminate the protocol; modify smart contracts; change fees, collateral parameters or eligible assets; control access to user interfaces; select or replace oracles; manage treasury assets; or otherwise determine essential features of the service.

Control exercised through admin keys, multi-signature arrangements, veto rights or emergency powers is particularly relevant.

The concentration of governance power should also carry significant weight. Formal DAO governance does not necessarily demonstrate decentralisation where voting rights are concentrated among founders, developers, affiliated entities or a small number of token holders. The assessment should consider effective voting power, delegation arrangements, quorum requirements, veto rights, proposal rights and whether governance decisions can realistically be implemented without the involvement of a core team.

The existence of custody may indicate intermediation where an identifiable person controls user assets, private keys or the smart contracts holding those assets. However, custody by the protocol itself should not be decisive. Crypto-assets may be locked in autonomous smart contracts without any person being able to control or transfer them unilaterally. The relevant question is who can exercise effective control over the assets or alter the conditions governing their use.

The fact that protocol code is not open source should not, by itself, determine whether a protocol is decentralised. Closed-source code reduces transparency and makes independent verification more difficult, but it does not necessarily establish the existence of an intermediary. Conversely, publishing source code does not demonstrate decentralisation where an identifiable person retains material control.

Marketing by an identifiable person or entity may indicate an ongoing commercial role, particularly where marketing is systematic, directed at EU users and combined with operation of the main interface, collection of fees or continued protocol development. Marketing alone should nevertheless not be decisive, as third parties may promote a protocol without controlling or providing the underlying service.

Additional criteria should include:

- control over the principal website, application or user interface;
- receipt of fees, revenues or other economic benefits from protocol use;
- control over treasury assets or economic incentives;
- responsibility for ongoing development and maintenance;
- control over oracles, bridges and other critical infrastructure;
- the ability to restrict access or determine which users, assets or transactions are permitted;
- reliance on an identifiable entity for the protocol's continued operation; and
- whether users reasonably rely on that entity for operation, support or remediation.

No single criterion should ordinarily be conclusive. The decisive question should be whether an identifiable person or coordinated group exercises sufficient legal, technical, governance or economic control to be regarded as providing the service. Only applications operating autonomously without such an intermediary throughout the relevant service chain should qualify as fully decentralised. This is necessary because DeFi arrangements may contain different degrees of centralisation across the settlement, protocol, application and interface layers.

Please explain your answers to question 61:

The assessment of whether a DeFi application is fully decentralised should follow a substance-over-form approach and consider the entire service chain and operational lifecycle. A protocol should not be considered fully decentralised merely because transactions are executed automatically through smart

contracts or because governance rights are formally assigned to token holders. DeFi arrangements may contain different degrees of centralisation across the protocol, application, governance and user-interface layers.

The existence of an identifiable intermediary providing the relevant crypto-asset service should be a primary criterion. Where an identifiable person or coordinated group operates the service, maintains an ongoing relationship with users or performs functions essential to its continued provision, the service should generally not be regarded as fully decentralised.

Similarly, control by an identifiable person or group over key protocol functionalities should carry substantial weight. Relevant forms of control include the ability to deploy, upgrade, pause or terminate the protocol; modify smart contracts, fees, collateral requirements or eligible assets; operate the main user interface; select or replace oracles; manage treasury assets; or restrict access. Admin keys, multisignature arrangements, veto rights and emergency powers are particularly strong indicators of effective control.

A significant concentration of governance power should also indicate that the application is not fully decentralised. Formal governance through a DAO or governance tokens is insufficient where effective control remains concentrated among founders, developers, affiliated entities or a small number of token holders. The assessment should consider voting-power concentration, delegation, quorum and proposal requirements, veto rights and whether governance decisions can be implemented without the involvement of a core team.

Custody of user assets by a protocol may be relevant but should not be decisive. Assets may be locked in smart contracts without any identifiable person having unilateral control over them. The relevant question is whether an identifiable person or group controls the assets, the private keys or the conditions governing their use.

The fact that protocol code is not open source should carry limited weight. Closed-source code reduces transparency and prevents effective independent verification, but does not necessarily demonstrate the existence of an intermediary. Conversely, open-source code does not establish decentralisation where an identifiable person retains control over key functions.

Marketing by an identifiable person or entity should be treated as a supporting indicator. It may demonstrate an ongoing commercial role where it is combined with control of the main interface, continued protocol development, fee collection or customer support. Marketing alone should not be conclusive, since a protocol may also be promoted by persons that do not control or provide the underlying service.

Additional relevant criteria should include:

- control over the main website, application or user interface;
- receipt of fees, revenues or other economic benefits from protocol use;
- control over treasury assets or economic incentives;
- responsibility for ongoing development, maintenance and cybersecurity;
- control over critical infrastructure, including oracles and bridges;
- the ability to restrict users, assets or transactions;
- reliance on an identifiable entity for continued operation; and
- users' reliance on an identifiable entity for support or remediation.

No single criterion should necessarily be conclusive. The overall assessment should determine whether an identifiable person or coordinated group exercises sufficient legal, technical, governance or economic control to be regarded as providing or controlling the relevant service. Only services operating autonomously and without such an intermediary throughout the relevant service chain should qualify as being provided in a fully decentralised manner and therefore fall outside MiCAR pursuant to Recital 22.

Question 62. Do you believe that risks to users of fully decentralised DeFi protocols should be indirectly accounted for by MiCA, e.g. by requiring CASPs to conduct due diligence over DeFi protocols they connect their clients with, or in any other way?

☒ Yes

☐ No

☐ Don't know / no opinion / not applicable

Question 62.1. Please specify how should MiCA account for risks from fully decentralised DeFi applications. For the purpose of this question, certification of a DeFi application should be understood as verifying that it robustly mitigates against smart contract vulnerabilities, operational risk in general and functions in accordance with its publicised performance:

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
CASPs should be able to connect their clients to any decentralised DeFi application, subject to giving appropriate warnings and disclosures on risks	☒	☐	☐	☐	☐	☐
CASPs should be liable for certain types of incidents when they have provided access to the relevant DeFi application and clients have been affected	☐	☐	☐	☒	☐	☐
CASPs should only facilitate connection of their clients to decentralised DeFi applications that are certified and service global (permissionless) liquidity	☐	☐	☐	☒	☐	☐
CASPs should only facilitate connection of their clients to decentralised DeFi applications that are certified and service only verified liquidity (verified pools)	☐	☐	☒	☐	☐	☐
CASPs should only facilitate connection of their clients to decentralised DeFi applications that service global	☐	☒	☐	☐	☐	☐

liquidity						
CASPs should be required to discontinue or discourage connecting clients to DeFi protocols that are strongly associated with illicit activity based on blockchain analytics	☐	☐	☐	☐	☒	☐
CASPs should not facilitate connection to decentralised DeFi applications	☒	☐	☐	☐	☐	☐
Public bodies should be required, or private organisations incentivised to publish whitelists or blacklists of DeFi protocols based on their risk profile	☐	☐	☒	☐	☐	☐
Other	☐	☐	☐	☐	☐	☒

Please specify to what other solution(s) you refer in your answer to question 62.1:

Please explain your answers to question 62.1, including your reasoning and any suggestions for improvement, recalibration, or alternative approaches:

MiCAR should not seek to regulate a fully decentralised DeFi application as if it were a legal person or intermediary. Where no identifiable person exercises control, conventional authorisation and organisational requirements cannot readily be imposed on the protocol itself. Instead, regulation should focus on identifiable regulated entities that facilitate access to DeFi, particularly CASPs integrating protocols into their interface, selecting protocols for clients, routing transactions or otherwise presenting DeFi access as part of their service.

CASPs should not be permitted to connect clients to any DeFi application subject only to warnings and disclosures. DeFi involves smart-contract vulnerabilities, oracle manipulation, governance attacks, private-key risks, fraud, complex value chains and significant information asymmetries. Risk disclosures alone do not adequately mitigate such risks.

A CASP facilitating access should conduct proportionate initial and ongoing due diligence on the relevant protocol. This should cover smart-contract audits, upgradeability and admin keys, governance concentration, oracle and bridge dependencies, operational history, liquidity, security incidents, economic design, conflicts of interest and exposure to illicit activity. Certification could support this assessment, but should not constitute a regulatory guarantee or replace the CASP's own obligations. Certification should be performed according to harmonised standards by independent and suitably qualified bodies and should be periodically renewed following material protocol changes.

Access should not necessarily be limited to verified liquidity pools. Permissionless global liquidity is a core feature of DeFi, and restricting CASPs exclusively to verified pools could substantially limit legitimate access and create closed EU-specific pools with insufficient liquidity. However, connection to global permissionless liquidity requires enhanced transaction monitoring, blockchain analytics and controls addressing illicit finance, sanctions, protocol

concentration and smart-contract risks.

CASP liability should depend on the CASP's role and the cause of the incident. A CASP should be liable where client losses result from its own acts or omissions, including deficient protocol selection or monitoring, misleading information, integration errors, inadequate cybersecurity, failure to act on known vulnerabilities or continuing to facilitate access despite material warning signs. A CASP should not automatically be liable for every autonomous protocol failure that could not reasonably have been identified or prevented. Liability should not be excluded through general contractual disclaimers.

CASPs should be required to discontinue or restrict access where reliable blockchain analytics and other evidence demonstrate a strong association with illicit activity, sanctions evasion, fraud or repeated security incidents. Decisions should be based on documented, objective and reviewable criteria rather than a single risk score or unverified allegation.

Public or private risk lists could provide useful supervisory intelligence, but a formal whitelist could create a misleading impression that listed protocols are safe or officially approved. Any such lists should therefore be dynamic, transparent as to methodology and legal effect, and subject to review and correction. They should support rather than replace each CASP's risk assessment.

Overall, MiCAR should establish proportionate obligations for CASPs facilitating DeFi access, including due diligence, ongoing monitoring, disclosures, record-keeping, conflicts management, incident response and clear responsibility for the CASP's own conduct. A general prohibition would be disproportionate and could drive users towards unregulated access channels, while unrestricted access based only on warnings would provide insufficient protection.

Please explain your answer to question 62:

Risks arising from fully decentralised DeFi protocols should be indirectly addressed under MiCAR where an authorised CASP actively facilitates or intermediates its clients' access to such protocols. Fully decentralised protocols may not have an identifiable operator to which conventional authorisation and supervisory requirements can be applied. However, this should not prevent requirements from applying to regulated intermediaries that select, integrate, promote or provide access to those protocols.

DeFi protocols may expose users to smart-contract vulnerabilities, oracle failures, governance attacks, price manipulation, liquidity risks, loss of assets and limited or absent legal recourse. Their complexity may also create significant information asymmetries, particularly for retail clients. EBA and ESMA have identified DeFi application interfaces, self-custodial wallets and centralised platforms as relevant access channels and highlighted ICT, money-laundering and consumer-protection risks associated with DeFi.

Where a CASP actively selects or integrates a DeFi protocol into its service offering, executes transactions with the protocol on behalf of clients, provides custody in connection with its use, or markets access to the protocol, the CASP should be required to conduct proportionate initial and ongoing due diligence. The assessment should cover, where relevant:

- the protocol's governance structure and the existence of persons exercising effective control or material influence;
- smart-contract audits, identified vulnerabilities and incident history;
- oracle design, dependencies and manipulation risks;
- liquidity, concentration and collateral risks;

- the degree of administrative control, including upgrade keys, emergency powers and the ability to amend or suspend the protocol;
- dependencies on developers, interfaces, bridges, validators and other critical third parties;
- tokenomics, incentive structures and conflicts of interest;
- legal, operational and AML/CFT risks; and
- arrangements for monitoring, suspension and orderly discontinuation of access.

CASPs should provide clients with clear, prominent and protocol-specific disclosures. These should explain that the protocol itself may not be authorised or supervised under MiCAR, that the client may have no identifiable counterparty or effective means of redress, and that the CASP's authorisation does not amount to regulatory approval of the DeFi protocol. Material smart-contract, governance, liquidity and loss risks should also be disclosed.

The intensity of the requirements should reflect the CASP's role. A CASP that actively selects, integrates or recommends a protocol should be subject to more extensive obligations than a CASP merely executing a client instruction. However, a disclaimer or characterisation of the service as "execution-only" should not remove the CASP's responsibilities where it has effectively curated, promoted or embedded the protocol in its own interface.

The framework should not require CASPs to guarantee the performance or security of decentralised protocols or impose responsibility for events genuinely outside their control. CASPs should nevertheless remain responsible for their own selection process, disclosures, technical integration, monitoring and response to identified risks. Where material deficiencies or unacceptable risks are identified, the CASP should restrict or discontinue facilitated access and inform affected clients.

At the same time, the requirements should not extend to situations in which clients independently access DeFi protocols through self-hosted wallets without any selection, intermediation or facilitation by a CASP. The regulatory connection should depend on the CASP's actual role and degree of control or influence.

Overall, indirect regulation through authorised CASPs is appropriate where CASPs function as gateways to DeFi. It would reduce regulatory gaps and improve client protection without treating the underlying fully decentralised protocol as if it were itself an identifiable regulated entity.

Question 63. Do you support introducing certification schemes for DeFi protocols and smart contracts?

- ☒ Yes, for all DeFi protocols and smart contracts providing any of the crypto-assets services defined under MiCA, and possibly also other services not in MiCA's scope such as lending and borrowing
- ☐ Yes for the DeFi protocols and smart contracts providing some of the crypto-assets services defined under MiCA
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 63, and explain for which types of DeFi services you support introducing certification schemes and for what reasons:

Certification schemes should be introduced for DeFi protocols and smart contracts that provide functions comparable to crypto-asset services under MiCAR, as well as for economically relevant services currently outside its scope, particularly crypto-asset lending and borrowing. A function-based approach is preferable because comparable technological and operational risks may arise irrespective of whether the relevant activity is already included in

Article 3(1), point (16), MiCAR.

Certification would be particularly appropriate for DeFi applications providing:

- exchange or trading functionalities;
- lending and borrowing;
- staking and liquid-staking services;
- custody-like or asset-management functionalities;
- portfolio management or automated investment strategies;
- transfer, settlement or payment functionalities; and
- services relying materially on bridges, oracles or interoperability arrangements.

These services may involve users committing crypto-assets to smart contracts, sometimes for extended periods or across interconnected protocols. Vulnerabilities may therefore result in significant and potentially irreversible losses. Relevant risks include coding errors, smart-contract exploits, manipulation of oracles, governance attacks, compromised admin keys, bridge failures and dependencies on other protocols. ESMA has identified important operational and security vulnerabilities in DeFi and noted the increasing complexity and interdependence of smart contracts.

Certification should verify, at a minimum:

- the security and integrity of the smart-contract code;
- independent audits and the treatment of identified vulnerabilities;
- upgradeability, admin keys and emergency intervention powers;
- governance arrangements and concentrations of control;
- dependencies on oracles, bridges and other protocols;
- operational resilience and incident-response mechanisms;
- the protection and technical treatment of user assets; and
- whether the protocol functions in accordance with its publicly stated design.

Certification should not constitute regulatory approval, confirm compliance with all applicable legal requirements or guarantee that users will not incur losses. It can provide assurance regarding defined technological and operational aspects at a particular point in time, but cannot eliminate protocol, market, liquidity or governance risks. The scope, date, methodology and limitations of certification should therefore be clearly disclosed.

Certification should be time-limited and renewed periodically and after material changes to the code, governance, critical dependencies or economic design. Harmonised EU standards should apply, and assessments should be carried out by independent and suitably qualified bodies subject to requirements concerning expertise, independence, conflicts of interest, transparency and professional liability.

Where a CASP selects, integrates or actively facilitates access to a DeFi application, certification should generally be required. However, it should complement rather than replace the CASP's own due diligence, ongoing monitoring and responsibility for the manner in which access is provided. The CASP should remain responsible for responding appropriately to material vulnerabilities, security incidents and changes to the protocol.

For fully decentralised applications accessed directly by users, mandatory certification may be difficult to enforce because no identifiable intermediary may exist. In such cases, voluntary certification could be encouraged. Certification could improve transparency and facilitate access through regulated CASPs without treating the fully decentralised protocol itself as a conventional regulated entity.

Please explain your answer to question 63:

Certification schemes could provide a useful minimum standard for assessing the operational and technological risks of DeFi protocols and smart contracts. This is particularly relevant given the risks arising from smart-contract vulnerabilities, governance attacks, oracle manipulation, dependencies between protocols and other operational and security weaknesses. ESMA has identified significant investor-protection, operational and security risks in DeFi and noted the increasing complexity and interdependence of smart contracts.

Certification should apply on a function-based basis. It should cover protocols and smart contracts performing functions comparable to crypto-asset services under MiCAR, as well as economically relevant activities currently outside its scope, particularly crypto-asset lending and borrowing. Limiting certification to activities already listed in MiCAR would leave material risks unaddressed merely because the underlying service is not yet included in the regulatory perimeter.

Certification should assess, at a minimum:

- the security and integrity of the smart-contract code;
- known vulnerabilities and the results of independent audits;
- upgradeability, admin keys and emergency intervention powers;
- governance arrangements and concentration of control;
- dependencies on oracles, bridges and other protocols;
- operational resilience and incident-response arrangements;
- the accuracy of publicly stated functionalities and performance;
- the handling and protection of user assets;
- material changes since the previous certification; and
- the availability of clear technical and risk documentation.

However, certification should not be understood as an approval of the protocol, a guarantee against losses or confirmation that the protocol complies with all applicable legal requirements. Smart contracts and their dependencies may change after certification, and vulnerabilities may emerge subsequently. Certification should therefore be time-limited, subject to periodic review and renewed following material changes to the code, governance, critical infrastructure or economic design.

The scheme should be based on harmonised EU standards and carried out by independent, suitably qualified and accountable certification bodies. Certification bodies should be subject to requirements concerning expertise, independence, conflicts of interest, methodology, professional liability and transparency. Certification results, scope, limitations, date and material findings should be publicly accessible.

Certification should be mandatory where an EU-authorised CASP selects, integrates or actively facilitates client access to a DeFi protocol as part of its

service. However, certification should not replace the CASP's own due diligence, ongoing monitoring or responsibility for the manner in which access is provided. The CASP should remain responsible for assessing whether the protocol is appropriate for integration and whether material changes, incidents or warning signs require access to be restricted or discontinued.

For fully decentralised protocols that are not connected to users through a regulated intermediary, mandatory certification may be difficult to enforce because there may be no identifiable person against whom the obligation can be applied. In such cases, voluntary certification should be incentivised through greater transparency and facilitated access through regulated CASPs.

Overall, certification could mitigate technological and operational risks and improve comparability. It should complement, rather than replace, regulation of identifiable intermediaries, CASP due diligence and clear risk disclosures.

Question 64. Which of the following statements about potential certification schemes of DeFi protocols do you agree with?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know No opinion Not applicable
Instead of a full CASP licence, DeFi protocols that are not fully decentralised should be required to obtain a certification before or soon after making the protocol available to the public	☒	☐	☐	☐	☐	☐
To obtain their certificate, DeFi protocols that are not fully decentralised should be required to integrate specific compliance tools in the design of their protocols	☐	☐	☐	☒	☐	☐
DeFi protocols and software developers offering the possibility to create and use non-custodial wallets should be required to obtain a certificate before making these wallets available to the public	☒	☐	☐	☐	☐	☐
DeFi protocols and software developers offering the possibility to create and use non-custodial wallets should be incentivised to obtain a certificate	☐	☐	☐	☒	☐	☐

Please explain your answers to question 64:

Certification should not replace authorisation under MiCAR where a DeFi protocol is not fully decentralised and an identifiable person or coordinated group provides a regulated crypto-asset service. The applicable regulatory treatment should follow the economic function of the activity and the degree of control exercised, rather than its technological form. Allowing certification instead of authorisation would create an unjustified alternative regime for services that

are functionally equivalent to those provided by CASPs and could encourage regulatory arbitrage.

Certification may nevertheless complement MiCAR authorisation. It could provide additional assurance regarding smart-contract security, operational resilience, admin keys, upgradeability, governance mechanisms and dependencies on oracles, bridges or other protocols. However, certification cannot replace requirements relating to governance, organisational substance, suitability of management, prudential safeguards, conflicts of interest, safeguarding of client assets and supervisory accountability.

Protocols seeking certification should, where technically and operationally appropriate, integrate compliance-supporting functionalities into their design. Depending on the relevant service and risk profile, these could include transaction-monitoring capabilities, sanctions-screening interfaces, access controls, audit trails, incident-management mechanisms, controls over protocol upgrades and emergency functions, and tools enabling the identification and management of illicit activity. Such requirements should be technologically neutral and proportionate and should not prescribe a single technical solution. They should also not create an expectation that technical tools alone ensure compliance with all legal obligations.

A mandatory certification requirement should not apply generally to the development and provision of non-custodial wallet software. Where developers merely publish software enabling users to create and control their own wallets, without holding private keys, executing transactions on behalf of users or otherwise providing a regulated service, mandatory certification would risk regulating software development irrespective of the existence of an intermediary. It could impose disproportionate barriers on open-source development and be difficult to enforce where software is developed collaboratively or outside the EU.

However, voluntary certification of non-custodial wallets should be encouraged. Certification could assess secure key generation and storage, transaction-signing processes, smart-contract permissions, recovery functions, software-update mechanisms, third-party dependencies and the accuracy of information provided to users. It could improve comparability and allow users and CASPs to identify wallets meeting recognised security standards.

Certification should be based on harmonised EU standards, carried out by independent and suitably qualified bodies, and renewed after material changes. Its scope and limitations should be clearly disclosed. Certification should not be presented as regulatory approval, a guarantee against losses or confirmation that the relevant protocol or wallet complies with every applicable legal requirement. ESMA has identified significant operational and security vulnerabilities in DeFi and increasing complexity and interdependence among smart contracts, which supports certification as a complementary risk-mitigation mechanism rather than a substitute for regulation.

Question 65. Which of the following statements about potential certification schemes of DeFi protocols or smart contracts do you agree with?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know No opinion Not applicable
Certificates should be issued by qualified private sector entities	☐	☐	☐	☒	☐	☐
Certificates should be issued by qualified public sector entities	☐	☒	☐	☐	☐	☐

Any interested party (e.g. persons providing connectivity to or participating in governance of DeFi protocols) should have the possibility to ask for the certification of a fully decentralised DeFi protocol	☐	☐	☐	☒	☐	☐
Only fully decentralised DeFi protocols that reach a certain significance (e.g. based on total value locked) should be required to obtain a certificate	☐	☐	☒	☐	☐	☐
CASPs should not be allowed to connect clients with DeFi protocols that are not certified	☐	☒	☐	☐	☐	☐

Please explain your answers to question 65:

Certification could contribute to greater transparency and more consistent assessments of DeFi protocols and smart contracts. DeFi arrangements may involve significant smart-contract, governance, oracle, liquidity, cybersecurity and operational risks. Their increasing complexity and interdependence make structured technical and risk assessments useful for CASPs, users and competent authorities.

Certificates should primarily be issued by qualified and independent private-sector entities with demonstrated expertise in smart-contract security, DLT systems and the economic risks of DeFi protocols. A public authority will generally not have the technical resources or operational capacity to audit and continuously reassess a large number of rapidly evolving protocols. Public authorities should instead establish or endorse minimum standards for certification, define eligibility and independence requirements for certifiers, maintain oversight of the certification framework and, where necessary, withdraw recognition from certifiers that fail to meet those standards.

Certification should assess more than the source code at a particular point in time. Depending on the protocol, its scope should include smart-contract security, governance and control mechanisms, upgrade and emergency powers, oracle dependencies, bridges and other critical infrastructure, external protocol dependencies, liquidity and concentration risks, tokenomics, incident history, administrator keys and procedures for responding to vulnerabilities. The certificate should clearly state its scope, methodology, date, version of the code assessed, identified limitations and period of validity.

Any interested party with a legitimate connection to the protocol should be able to request certification, including developers, governance participants, interface providers and CASPs facilitating access. As fully decentralised protocols may not have a legal person or identifiable operator capable of applying for certification, restricting applications to protocol operators would make certification unavailable precisely where it may be most relevant.

Mandatory certification could be considered for protocols reaching a defined level of significance. However, total value locked should not be the sole criterion, as it is volatile and may not adequately reflect risks to EU users. Relevant indicators could also include the number of EU users, transaction volumes, interconnectedness, use by regulated entities, concentration of assets, leverage and the potential impact of a protocol failure. The mechanism for imposing a certification obligation must nevertheless account for the absence of an identifiable person that can legally be required to apply for certification. Where no such person exists, additional obligations may need to apply to CASPs facilitating access rather than directly to the protocol.

CASPs should not be subject to an absolute prohibition on connecting clients with uncertified protocols. Such a prohibition could effectively make a private certificate a mandatory market-access authorisation, restrict access to innovative or newly established protocols and create substantial barriers to entry. It

could also result in excessive concentration among a small number of certified protocols and certification providers.

Instead, certification should form part of the CASP's risk-based due diligence, as outlined in our response to Question 62. Access to an uncertified protocol should require enhanced due diligence, more prominent client warnings and, where appropriate, restrictions for retail clients. CASPs should not facilitate access where they cannot obtain sufficient information to assess the protocol or where material risks cannot be adequately managed.

Finally, certification must not be presented as a guarantee that a protocol is secure or that losses cannot occur. A technical assessment is necessarily limited to a defined codebase, scope and point in time. Protocol upgrades, governance decisions, external dependencies and newly identified vulnerabilities may subsequently alter the risk profile. Certification should therefore be time-limited, subject to reassessment following material changes and supported by ongoing monitoring.

4.2 Staking, lending and borrowing of crypto-assets

This section seeks stakeholders' feedback on staking, lending and borrowing of crypto-assets, currently not addressed in MiCA regulation ([EBA-ESMA joint report on recent developments in crypto-asset markets - January 2025](#)). Staking is the process of immobilising crypto-assets to support the operations of proof-of-stake and proof-of-stake-like blockchain consensus mechanisms in exchange for the granting of validator privileges that can generate block rewards. The provision of staking services often implies that the crypto-assets, or the private keys giving access to them, are held by the staking service provider in custody. Thus, the provision of staking services is ancillary to custody services which are fully covered under MiCA. The provision of staking services therefore requires that the staking service provider is authorised under MiCA to provide custody and administration of crypto-assets on behalf of clients, as set out in Article 75 MiCA. Furthermore, CASPs should obtain an explicit consent from the clients to stake their crypto-assets, as it may have an impact on their clients' ability to access them.

Respondents are asked to provide concrete examples to support answers provided, and, where possible, quantitative and qualitative information.

Question 66. Do you think the current approach whereby staking services are not separately regulated is adequate?

☐ Yes

☒ No

☐ Don't know / no opinion / not applicable

Please explain your answer to question 66:

As stated in our response to Question 46, staking services provided on behalf of clients should be expressly included in the catalogue of crypto-asset services under MiCAR.

The current approach, under which staking is treated primarily as ancillary to custody, does not adequately reflect the specific risks and different forms of staking services. While staking frequently involves custody of clients' crypto-assets or control over the relevant private keys, this is not necessarily the case for all staking models. Moreover, authorisation for custody does not by itself comprehensively address staking-specific risks and obligations.

A dedicated regulatory framework should apply where a service provider stakes crypto-assets on behalf of clients, pools client assets, selects or operates validators, exercises discretion regarding the staking process, or receives and distributes staking rewards. The requirements should cover, in particular:

- the client's prior and explicit consent;
- custody, segregation and the legal ownership of staked crypto-assets;
- lock-up and unbonding periods and the resulting restrictions on availability;
- slashing, validator, protocol, operational and liquidity risks;
- the selection, monitoring and concentration of validators;
- the calculation and distribution of rewards;
- all fees, commissions and retained rewards;
- the provider's liability for losses or operational failures;

- the treatment of staked assets and rewards in the event of insolvency; and
- business continuity and orderly termination of the service.

Clients should be clearly informed whether rewards are generated by the relevant protocol, whether their amount is variable, whether the service provider guarantees any return, and which party bears the risk of slashing or other losses. MiCAR should also distinguish between custodial staking, non-custodial staking, delegated staking and services involving only the provision of technical infrastructure. Purely technical activities without control over client assets or an ongoing client relationship should not automatically be subject to the same requirements as custodial staking services.

The regulatory treatment should be based on the substance of the activity and the degree of control exercised by the service provider, rather than solely on whether the service is formally combined with custody. This would ensure consistent client protection while avoiding the disproportionate regulation of genuinely decentralised or purely technical participation in proof-of-stake networks.

Where staking services are brought within the regulatory perimeter, appropriate transitional measures should be provided for existing business models. Providers should have sufficient time to obtain or extend their authorisation and adapt their contractual, organisational and technical arrangements. Such measures should ensure timely client protection without unnecessarily disrupting viable existing businesses.

What specific requirements should be applied to staking service providers?

Staking-as-a-service should be explicitly recognised as a crypto-asset service under MiCAR and subject to proportionate requirements addressing its specific risks. The framework should apply where an intermediary stakes crypto-assets on behalf of clients or exercises discretion or control over the staking process, but not to holders staking their own crypto-assets directly.

Under the current interpretation, staking involving custody of clients' crypto-assets or private keys is treated as ancillary to custody and administration under Article 75 MiCAR. Providers must therefore comply with MiCAR's general and custody-related requirements. However, MiCAR does not contain rules specifically addressing staking risks.

A dedicated framework should include the following elements:

1. Prior and explicit client consent

CASPs should obtain explicit client consent before staking assets. Consent should be separate from the custody agreement and disclose whether the CASP acts as validator, delegates to a third-party validator or uses a staking pool. Material changes should require renewed consent.

2. Staking agreement and disclosures

The agreement should define the parties' rights and obligations and disclose the staking arrangement, lock-up and unbonding periods, unstaking conditions, reward methodology, fees, risks, liability allocation and the treatment of assets in the event of insolvency or termination. Information on rewards must be fair, clear and not misleading. Estimated or historical rewards should not be presented as guaranteed returns.

3. Protection and segregation of client assets

Staked assets and rewards should remain attributable to the client and be segregated from the CASP's own assets. CASPs should maintain records of ownership, amounts staked, rewards accrued and deductions made. Client assets must not be used for the CASP's own account.

4. Slashing and liability

CASPs should be liable where slashing-related losses result from their acts or omissions, including inadequate validator selection, monitoring failures or non-compliance with protocol requirements. Liability for protocol-wide events outside the CASP's control may be limited where risks have been clearly disclosed.

5. Validator and protocol due diligence

CASPs should establish documented criteria for selecting and monitoring validators, staking pools and protocols. Assessments should cover operational resilience, technical performance, cybersecurity, governance, concentration risks, conflicts of interest and legal enforceability. Excessive concentration (e.g. with individual validators, protocols or infrastructure providers) should be avoided.

6. Liquidity and unstaking arrangements

CASPs should disclose that staked assets may be unavailable during lock-up and unbonding periods and maintain procedures for processing unstaking requests within protocol timelines. Where immediate access is offered despite an unbonding period, the resulting liquidity risk should be subject to additional risk-management and prudential requirements.

7. Governance and operational resilience

CASPs should maintain adequate expertise, systems and controls for staking operations. Responsibilities for validator selection, monitoring, reward calculation and incident management should be clearly allocated. Delegated staking functions should be treated as outsourcing and should not reduce the responsibility of the authorised CASP.

8. Conflicts of interest

CASPs should identify and manage conflicts arising from affiliated validators, protocol selection, reward retention or the allocation of staking opportunities. Clients should receive fair treatment in the allocation of rewards and losses.

9. Record-keeping and reporting

CASPs should maintain records of assets staked, validators and protocols used, rewards distributed, fees deducted, unstaking requests, slashing events and material operational incidents. Competent authorities should receive proportionate reporting on material volumes, concentrations, third-party dependencies and complaints.

10. Proportional prudential treatment

Additional own-funds or insurance requirements should be considered where a CASP assumes liability for slashing, guarantees rewards or liquidity, advances assets during unbonding periods or otherwise assumes principal, credit or liquidity risk. Purely technical or administrative staking services should not automatically attract the same treatment.

Overall, the framework should distinguish between direct staking, non-custodial technical services and intermediated staking-as-a-service. Existing MiCAR requirements should not be duplicated but complemented by targeted rules on consent, disclosures, validator selection, slashing, rewards, liquidity and unstaking.

Question 67. Do you think that lending and borrowing of crypto-assets should be regulated?

☒ Yes

☐ No

☐ Don't know / no opinion / not applicable

What do you believe should be the main elements of regulatory requirements applicable to lending and borrowing and why?

Authorisation and regulatory perimeter: Crypto-asset lending and borrowing should be included in the list of crypto-asset services under MiCAR. Clear criteria should distinguish between lending and borrowing activities, ancillary activities and cases where a CASP merely facilitates access to third-party or decentralised protocols. Economically equivalent activities should not receive different regulatory treatment solely because of their technical structure.

Clear contractual terms and disclosures: CASPs should provide clients with clear information on the legal nature of the arrangement, including whether ownership of crypto-assets is transferred, whether clients retain proprietary rights or only contractual claims, and whether they bear borrower or CASP default risk. Terms should also cover duration, withdrawal rights, yield calculation, fees, collateral requirements, margin calls, liquidation procedures, default arrangements and insolvency treatment.

Advertised yields should not be described as guaranteed or risk-free unless supported by a legally enforceable guarantee and adequate financial resources. Any distinction between fixed, variable and estimated returns should be clearly disclosed.

Client asset protection: Clients should provide explicit consent before their crypto-assets are lent, pledged, transferred, rehypothecated or otherwise used. CASPs should maintain accurate records regarding ownership, use and status of assets.

Rehypothecation and collateral chains should either be restricted or subject to strict safeguards, including transparency, concentration limits, risk controls and explicit client consent. Assets used in lending arrangements should be clearly distinguished from assets held in custody under Article 75 MiCAR.

Credit, counterparty and concentration risk management: CASPs should conduct appropriate credit and counterparty assessments and establish limits for counterparties, affiliated entities, collateral types and connected groups. Material intra-group exposures should be identified and managed under the same standards as external exposures.

Collateral and liquidation requirements: Where lending is collateralised, CASPs should apply prudent valuation methodologies, haircuts, collateral eligibility criteria and margin requirements reflecting volatility, liquidity and concentration risks. Clients should be informed of margin-call and liquidation procedures. Liquidations should be conducted fairly and minimise avoidable losses and market disruption.

Liquidity and maturity risk management: CASPs should manage mismatches between the maturity and liquidity of assets and liabilities. Where clients are promised immediate or short-term access to crypto-assets that have been lent for longer periods, adequate liquidity resources and contingency arrangements should be maintained. Withdrawal terms should accurately reflect underlying liquidity.

Governance and conflicts of interest: CASPs should maintain adequate expertise, systems and controls for lending and borrowing activities. Particular attention should be given to conflicts arising from lending to affiliated entities, acting simultaneously as lender, borrower and intermediary, setting collateral valuations or having an economic interest in certain borrowers or assets. The authorised CASP should retain sufficient organisational substance and effective control, including where functions are outsourced or performed within a group.

Prudential safeguards: Additional own-funds, liquidity or insurance requirements should apply where a CASP lends from its own balance sheet, borrows from clients, guarantees repayment or yield, assumes counterparty risk or provides liquidity despite maturity mismatches. Prudential requirements should reflect lending volumes, leverage, unsecured exposures, collateral quality, concentration and interconnectedness.

Client classification and investor protection: Retail clients should receive enhanced protection, including prominent risk warnings and, where appropriate, appropriateness assessments. This would require a harmonised distinction between retail and non-retail clients under MiCAR.

Reporting and supervisory transparency: CASPs should report material lending and borrowing volumes, major exposures, collateral composition, leverage, liquidity mismatches, defaults, liquidations, rehypothecation practices and client complaints. Reporting should be proportionate and avoid duplication with other Union legislation.

Overall, regulation should focus on the economic substance and risks of the activity rather than its label or technical implementation. Existing MiCAR requirements relating to custody, governance, outsourcing, conflicts of interest and operational resilience should not be duplicated but complemented by targeted rules addressing credit, counterparty, collateral, leverage, liquidity and investor-protection risks arising from crypto-asset lending and borrowing.

Please explain your answer to question 67:

Crypto-asset lending and borrowing should be expressly regulated under MiCAR. As noted in our responses to Questions 45 and 57, these activities constitute an important product line for a number of CASPs but are not currently included as separate crypto-asset services under Article 3(1), point (16), MiCAR. Where lending or borrowing is combined with custody or another regulated crypto-asset service, only parts of the overall product may fall within the MiCAR framework. This creates legal uncertainty regarding the regulatory perimeter and may give clients the misleading impression that the entire product is subject to MiCAR safeguards.

Crypto-asset lending and borrowing entail specific risks that are not adequately addressed by the requirements applicable to related crypto-asset services. These include counterparty and credit risk, liquidity and maturity mismatches, collateral volatility, leverage, forced liquidations, rehypothecation, concentration risk, conflicts of interest and operational risks. EBA and ESMA have also identified information asymmetries, excessive leverage and potential systemic risks arising from collateral chains, procyclicality and interconnectedness. In particular, users may receive insufficient information on fees, interest rates or yields, changes to collateral requirements and their contractual rights and obligations.

The regulatory framework should be technology-neutral and function-based. It should distinguish between lending by a CASP from its own balance sheet, intermediation between lenders and borrowers, arrangements under which clients make crypto-assets available to the CASP in return for a yield, and services facilitating access to lending protocols. The applicable requirements should reflect whether the CASP acts as principal, agent or intermediary and whether the CASP assumes credit, liquidity or principal risk.

4.3 Non-fungible tokens

Under MiCA Article 2(3), crypto-assets that are unique and not fungible with other crypto-assets (NFTs) are out of the scope of the regulation.

Question 68. In your view, does the current state of the NFT market and the risks and opportunities associated with it justify regulating providers of services related to these tokens?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

What do you believe should be the main elements of regulatory requirements applicable to NFTs?

Any regulatory requirements applicable to NFTs should follow a technology-neutral, proportionate and substance-over-form approach. The first step should be a clear classification assessment. Where an NFT qualifies as a financial instrument, forms part of an AIF or falls within another existing regulatory framework, that framework should apply instead of MiCAR. For example, an NFT-based arrangement may qualify as an AIF where capital is raised from several investors and invested according to a defined investment policy for their benefit.

Additional requirements should therefore focus on genuine NFTs and related professional services that would otherwise remain outside the regulatory perimeter. The main elements should include:

1. Clear classification criteria

The framework should clarify when a token is genuinely unique and non-fungible. The assessment should consider its economic function, embedded rights, substitutability and actual use rather than its technical identifier or designation as an NFT. Particular attention should be paid to large series or collections, fractionalised NFTs and tokens with substantially identical characteristics or investment features.

2. Information and disclosure

Purchasers should receive clear, fair and non-misleading information on:

- the identity and role of the issuer, offeror and relevant service provider;
- the rights represented by the NFT;
- whether ownership, intellectual-property rights, access rights or only contractual claims are transferred;
- fees, royalties and other charges;
- technological, custody, liquidity and valuation risks;
- the location and availability of the referenced asset or digital content; and
- the consequences of platform discontinuation, insolvency or loss of access to off-chain content.

NFTs should not be marketed as investments with guaranteed value or returns where no legally enforceable basis exists.

3. Requirements for professional service providers

Professional NFT marketplaces, custodians and intermediaries should be subject to requirements proportionate to their activities. These should cover governance, operational resilience, cybersecurity, safeguarding and segregation of client assets and funds, conflicts of interest, complaints handling and record-keeping. Where a provider performs a function economically equivalent to a crypto-asset service under MiCAR, comparable requirements should apply unless another EU framework already governs the activity.

4. Market integrity

NFT marketplaces should maintain arrangements to detect and prevent fraud, wash trading, self-dealing, misleading bidding practices and manipulation of prices or trading volumes. Material conflicts of interest, proprietary transactions and arrangements affecting the ranking or visibility of NFTs should be disclosed.

5. Custody and asset protection

Where a provider holds NFTs, private keys or client funds, safeguarding, segregation and reconciliation requirements should apply. Contracts should clearly allocate responsibility for loss, theft, unauthorised transfers, technical failures and provider insolvency.

6. Link to the underlying asset

The legal and technical relationship between the NFT and any referenced asset or content should be transparent. Providers should disclose whether content is stored on-chain or off-chain, who is responsible for maintaining access and whether the NFT can retain its intended functionality if an external platform, server or issuer ceases operating.

7. Proportionality

The full CASP framework should not automatically apply to artists, creators or owners making occasional sales of genuinely unique NFTs without providing intermediary services professionally. Requirements should be calibrated according to the nature, scale and risks of the service. Overall, existing sectoral legislation should take precedence whenever its conditions are met. Any additional regime should close residual regulatory gaps, ensure consistent treatment of functionally equivalent services and avoid overlaps between MiCAR, MiFID II, AIFMD and other applicable legislation.

Please explain your answer to question 68:

Providers of services related to NFTs should be subject to proportionate regulation where their activities create risks comparable to those addressed by MiCAR and are not already governed by other EU or national legislation.

The exclusion of genuinely unique and non-fungible crypto-assets from MiCAR does not mean that NFT-based arrangements are necessarily unregulated. Depending on their structure, economic function and the rights attached to the token, they may qualify as financial instruments or form part of a collective investment undertaking. For example, an arrangement may qualify as an AIF where capital is raised from a number of investors and invested according to

a defined investment policy for their benefit. ESMA has confirmed that this assessment must be conducted on a case-by-case basis and that undertakings investing in crypto-assets may qualify as AIFs where the relevant AIFMD criteria are met (ESMA75453128700-1323).

Similarly, NFTs may qualify as transferable securities, units in collective investment undertakings, derivatives or other financial instruments where their characteristics and attached rights meet the applicable criteria. In such cases, MiFID II, AIFMD or other relevant sectoral legislation should apply. The classification must follow a technology-neutral, substance-over-form approach. The NFT label or use of a unique technical identifier should not determine the applicable regime.

Any additional regulation under MiCAR should therefore focus on residual regulatory gaps. In particular, it could cover professional providers operating marketplaces, providing custody, executing transactions or transferring genuine NFTs where comparable intermediary activities would otherwise remain outside both MiCAR and other financial-services legislation.

The framework should avoid overlapping regulation and should not automatically apply the full CASP regime to occasional sales by artists, creators or owners of genuinely unique NFTs. Requirements should be proportionate to the nature, scale and risks of the service and could address governance, asset safeguarding, operational resilience, conflicts of interest, fee transparency, complaints handling and market abuse.

Clearer guidance is also needed to distinguish genuine NFTs from large collections, fractionalised NFTs and other arrangements that display economic fungibility or investment characteristics. Overall, existing sectoral frameworks should apply first where their conditions are met. Additional MiCAR regulation should address only services presenting comparable risks that would otherwise remain outside the regulatory perimeter.

4.4 Prediction markets and perpetual futures

One of the most marked developments in crypto markets since MiCA was adopted is the emergence of DLT-based prediction markets and the volume of trading activity in perpetual futures on crypto-assets.

Prediction markets where parties take a bet on a future development in almost any area, often far removed from financial assets or services, are increasingly conducted on or are structured through DLT, smart contracts and crypto-assets.

Question 69. Do prediction markets present opportunities or risks for EU consumer and investors?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please elaborate on your answer to question 69:

- Prediction markets are often functionally identical to binary options, the marketing, distribution and sale of which to retail clients are already prohibited under existing product intervention measures. Beyond the risks posed to retail investors, including gambling-related harms, such products may create incentives for the misuse of insider information and for influencing or manipulating the occurrence or outcome of the underlying event (for example, morally objectionable bets on forest fires could create incentives for the deliberate ignition of forest fires).
- If prediction markets qualify as binary options and are therefore generally prohibited, a legislative clarification to that effect would be desirable.

Question 70. Should prediction markets, where they are DLT enabled and facilitated through smart contracts be governed by MiFID or MiCA?

- ☐ By MiFID
- ☐ By MiCA
- ☒ Don't know / no opinion / not applicable

Please explain your answer to question 70:

- If the applicability of MiFID/MiCAR is determined by reference to the underlying asset/event of the product or settlement, a dedicated regulatory framework should be considered, potentially independent of both MiCAR and MiFID, to address any resulting regulatory gap.
- Additionally, if possible, clear criteria are needed to distinguish prediction markets from betting activities.

Question 71. What substantive requirements should be considered for service providers that provide prediction market services?

For consumer protection purposes, a dedicated framework should include restrictions on eligible underlying events/asset and outcomes (certain outcomes, particularly those that are contrary to public policy or morality, such as wars, forest fires, or deaths, should be prohibited as underlying events.), limitations on marketing and distribution, product governance requirements, restrictions on the target market, obligations to monitor market abuse, and compensation

requirements where the underlying event or outcome is subsequently found to have been manipulated. The regulatory classification of prediction markets should follow the principle of “substance over form”. The use of DLT, smart contracts or crypto-assets for issuance, trading or settlement should not determine the applicable regulatory framework. Where an event contract meets the criteria of a financial instrument, notably a derivative or binary option under Section C of Annex I to MiFID II, it should remain governed by MiFID II and should not be brought within MiCAR merely because it is implemented through DLT. ESMA has similarly clarified that event contracts with binary payouts qualify as financial instruments where the underlying falls within the categories listed in Section C(4) to (10) of Annex I to MiFID II.

This approach preserves the established boundary between MiFID II and MiCAR, avoids regulatory arbitrage and ensures that functionally equivalent products are subject to equivalent requirements. Otherwise, providers could potentially alter the applicable regime solely by tokenising a product or using smart contracts, although its economic substance and risk profile remain unchanged.

However, not all prediction markets or event contracts necessarily qualify as financial instruments. Classification should therefore be conducted on a case-by-case basis, considering the contractual structure, payout mechanism, tradability, settlement method and nature of the underlying event. Event contracts that do not qualify as financial instruments may instead fall within national gambling law. Only where a token-based arrangement neither constitutes a financial instrument nor falls under another applicable regulatory framework should its possible treatment under MiCAR be considered. ESMA has also recognised that event contracts may, depending on their characteristics, qualify as financial instruments, gambling products or, where issued in token form and not constituting financial instruments, crypto-assets under MiCAR.

Accordingly, MiFID II should govern DLT-enabled prediction markets to the extent that the relevant event contracts qualify as financial instruments. The use of DLT or smart contracts should remain technologically neutral and should not lead to a different legal classification.

Question 72. Should perpetual futures on crypto-assets and services towards such perpetual futures be governed by MiCA or MiFID.

- ☐ By MiFID
- ☐ By MiCA
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 72:

Question 73. What substantive requirements should be considered for perpetual futures on crypto-assets and service providers providing service for such perpetual futures?

- Regarding collective consumer protection:
- leverage and margin requirements
- transparent pricing and funding mechanisms
- robust risk management
- effective conflict-of-interest controls
- clear and transparent customer information
- robust product-governance requirements; including an assessment of whether the product is appropriate for the intended target market; particular attention should be paid to retail clients

4.5 Tokenised deposits

The terms ‘tokenised deposit’ and ‘deposit tokens’ are not defined terms and are sometimes used interchangeably ([EBA Report on tokenised deposits - December 2024](#)). For the purposes of the following questions, ‘tokenised deposits’ are digital representations of traditional commercial bank deposits recorded on a blockchain or distributed ledger, allowing for programmable, instant 24/7 settlements.

Question 74. Tokenised deposits could be deployed in support of a range of use cases across payments, capital markets, and on-chain financial activities. Based on your experience and expectations, please assess the potential relevance and benefit of tokenised deposits for each of the following use cases in the EU:

	1 (not relevant / no meaningful benefit)	2 (low relevance / limited benefit)	3 (moderate relevance / moderate benefit)	4 (high relevance / high benefit)	5 (very high relevance / transformative benefit)	Don't know - No opinion Not applicable
Person to person payments	☒	☐	☐	☐	☐	☐
Retail POI payments (domestic, day-to-day point of interaction transactions)	☒	☐	☐	☐	☐	☐
Intra-EU cross-border payments (non-POI)	☒	☐	☐	☐	☐	☐
International payments and remittances (third countries)	☐	☐	☒	☐	☐	☐
Settlement of tokenised securities and other financial instruments	☐	☐	☐	☒	☐	☐
Delivery-versus-payment (DvP) and atomic settlement	☐	☐	☐	☒	☐	☐
Intraday liquidity management (real-time funding and liquidity optimisation)	☐	☐	☒	☐	☐	☐
Treasury and liquidity management services for corporates and financial institutions	☐	☐	☒	☐	☐	☐
Programmable payments and smart-contract-based use cases	☐	☒	☐	☐	☐	☐
On-chain collateral or margining in regulated markets	☐	☐	☒	☐	☐	☐
Improved settlement speed and operational efficiency	☐	☐	☒	☐	☐	☐
Reduction of counterparty and settlement risk	☐	☐	☐	☒	☐	☐

Please explain your answers to question 74:

The FMA considers that DeFi applications currently present only limited interest and relatively limited adoption in the area of payment and transaction services.

While payment use cases are frequently cited as one of the key advantages of blockchain-based systems, practical adoption remains limited. In many cases, existing payment infrastructures already provide efficient solutions for domestic and regional payments. Within the EU, for example, SEPA Instant already enables near real-time payments with strong legal certainty and high operational reliability.

Moreover, many of the benefits traditionally associated with blockchain-based payment systems can increasingly be achieved through interoperability solutions connecting DLT-based infrastructures with existing payment systems and central bank settlement infrastructure. As a result, there is currently limited evidence that DeFi-based payment applications provide a sufficiently compelling advantage to drive widespread adoption.

The FMA further notes that much of the crypto-asset ecosystem has become increasingly intermediary-driven, with users relying on CASPs and other service providers rather than interacting directly with decentralised protocols. This reduces some of the originally anticipated disintermediation benefits of DeFi in the payments context.

The FMA considers that DeFi applications may offer important potential benefits in the area of exchange services, particularly through automated market making, continuous market access and cross-border accessibility.

However, adoption remains limited relative to the broader financial system and significant weaknesses remain, including concerns relating to governance, market integrity, operational resilience, legal certainty and investor protection.

The FMA considers that DeFi applications may offer important potential benefits for trading and investment-related activities, particularly in tokenised environments and for certain crypto-native assets.

Nevertheless, use remains relatively concentrated within the crypto-asset sector. The long-term viability of these models outside the crypto ecosystem remains uncertain, particularly where similar functionalities may be achieved through regulated financial market infrastructures or future DLT-enabled settlement solutions.

The FMA considers that current DeFi lending and borrowing applications remain of limited interest. While the underlying technology may present innovative features, adoption remains relatively limited and significant weaknesses persist, including liquidity risks, procyclicality, collateral management risks, governance concerns and the absence of clearly identifiable responsible entities.

The FMA considers that DeFi-related custody solutions are already used to a significant extent within the crypto-asset ecosystem. However, important risks and weaknesses remain, particularly regarding key management, operational security, smart-contract vulnerabilities and the allocation of liability in the event of loss or technical failure.

Many of the theoretical advantages historically attributed to DeFi and blockchain-based payment systems remain largely unproven in practice. Where genuine efficiency gains exist, particularly in wholesale financial market infrastructures, similar outcomes may increasingly be achievable through DLT-

enabled interoperability solutions and central bank settlement infrastructures without requiring the broader migration of payment and transaction services to fully decentralised environments.

Question 75. Please select one or two use cases and benefits above that you consider most promising in the EU:

Maximum 2 selection(s)

- ☐ Person to person payments
- ☐ Retail POI payments (domestic, day-to-day point of interaction transactions)
- ☐ Intra-EU cross-border payments (non-POI)
- ☐ International payments and remittances (third countries)
- ☒ Settlement of tokenised securities and other financial instruments
- ☐ Delivery-versus-payment (DvP) and atomic settlement
- ☐ Intraday liquidity management (real-time funding and liquidity optimisation)
- ☐ Treasury and liquidity management services for corporates and financial institutions
- ☒ Programmable payments and smart-contract-based use cases
- ☐ On-chain collateral or margining in regulated markets
- ☐ Improved settlement speed and operational efficiency
- ☒ Reduction of counterparty and settlement risk

Please explain why the case(s) you selected in your answer to question 75 are the most promising in the EU:

See above Q 74

Question 76. What factors, if any, constrain the development and uptake of tokenised deposits in the EU?

Question 77. If you identify any regulatory issue(s) in your answer to the previous question, please indicate what regulatory action is appropriate to address the issue(s) identified:

The FMA considers that the main regulatory challenge regarding tokenised deposits is not the prudential treatment of deposits, but rather their classification.

At present, the concept of a deposit is not fully harmonised across the relevant EU legislative frameworks, including the CRD and the Deposit Guarantee Schemes framework. This gives rise to legal uncertainty and creates boundary issues with MiCA, particularly in relation to tokenised representations of

bank liabilities.

The FMA therefore considers that the primary policy objective should be to establish a more harmonised and technology-neutral understanding of what constitutes a deposit. If a token merely represents a deposit claim against a credit institution, the existing prudential framework for deposits is generally sufficient and does not require fundamental modification solely because the claim is recorded or transferred using DLT.

Accordingly, the FMA does not currently see a need for a dedicated prudential regime for tokenised deposits. Greater legal clarity regarding classification would be significantly more important than the introduction of new regulatory requirements.

At the same time, the European Commission should carefully consider the boundary between deposits and emerging crypto-asset or DeFi-related activities. Certain arrangements may exhibit characteristics that resemble deposits while incorporating additional features such as staking-like rewards, yield-generation mechanisms or other investment-like functionalities. The Commission should clarify whether, and to what extent, such features remain compatible with the concept of a deposit.

More generally, the FMA considers that the key policy question is not whether deposits should be permitted on DLT, but rather where the boundary between banking activities and DeFi-based financial services should be drawn. Where licensed credit institutions merely tokenise traditional deposits, the existing regulatory framework appears broadly adequate. Further harmonisation and clarification of the deposit concept would therefore be preferable to the creation of a new bespoke regulatory regime.

Question 78. Do tokenised deposits raise any specific issues under the CRD/CRR framework?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please indicate what issues arise and what regulatory or supervisory action may be appropriate to address the issue(s) identified:

See Q 77

Please explain your answer to question 78:

Question 79. Do tokenised deposits raise any questions and challenges from a deposit insurance perspective?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please indicate which supervisory or regulatory action is appropriate to address the issues identified:

See Q 77.

Please explain your answer to question 79:

4.6 Legal treatment of tokens

Legal certainty in the treatment of tokens in the EU and in the Member States is crucial in supporting predictable outcomes in financial markets in Europe and is vital to avoid stifling innovation, both in relation to MiCA crypto-assets (crypto-assets) as well as for the tokenisation and issuance of financial instruments in the form of tokens, currently governed by MiFID/R or asset management regulation (DLT financial instruments). Tokens in this section generally refer to both DLT financial instruments and crypto-assets, unless specified otherwise. In relation to legal certainty in the treatment of tokens, at least several issues have been noted by stakeholders, supervisors and academics. These include questions on whether tokens can be objects of property, which rules apply to the title and transfer of tokens, their treatment in the event of insolvency, custody relationships, and security rights in crypto-assets.

There are different ways to categorise tokens depending on the type of rights they confer to the holder. There are two general types of tokens, native tokens and non-native tokens. Native tokens tend to represent an asset (such as a share or security) that **only exists on-chain** (i.e. without a physical or traditional paper-based equivalent). Non-native tokens tend to **represent an on chain right over an asset that is legally constituted and represented elsewhere (off chain)** allowing this right to be held and transacted on DLT. Regarding non-native tokens, legal uncertainties may arise because, depending on the legal framework and the way the token was created, the tokenisation often leads to the simultaneous existence of two assets: the token representing the asset and the asset that the token asset represents^[4]. Native tokens too may raise important legal questions about their nature as many jurisdictions of today do not explicitly recognise existence of on-chain assets and it is often unclear if and how they fall under current rules on taxonomy and creation of traditional financial assets.

One of the key questions concerning legal certainty is whether holding (or controlling) a token on a blockchain constitutes ownership, and whether holding (or controlling) a non-native token constitutes ownership or merely a claim on the underlying asset that it represents. MiCA contains clear requirements for issuers or offerors of crypto-assets but it does not directly regulate the ownership of such assets, which remains a matter of (national) property laws. Similarly, MiFID does not define the proprietary nature of financial instruments or transfer of ownership, which is left to the discretion of national laws. Some Member States have implemented specific regulations to ensure legal certainty for tokens, including to provide for statutory “bridges” that synchronise the technical state of the ledger with the legal status of the asset.

^[4] In “complete tokenisation” possession can equate to legal ownership over the asset it represents if the legal system recognises the token as the asset’s representation; the “indirect tokenisation” where the legal ownership depends on the intermediary entity or legal structure, not just the token; and the “incomplete tokenisation” where the token might only act as evidence or an interface to rights that are legally held off-chain. [X. Lavayssière, “Legal Structures of Tokenised Assets”. European Journal of Risk Regulation.](#)

Question 80. Is there legal uncertainty as to the private law treatment of issuance, holding and transfers of tokens, under national law?

- ☒ Yes
- ☐ No
- ☐ Don’t know / no opinion / not applicable

Question 80.1. Which of the following issues are most significant?

	1 (none or not significant)	2 (low)	3 (moderate)	4 (high)	5 (very high)	Don't know No opinion Not applicable
Issuing a crypto-asset token in compliance with national law	☐	☐	☒	☐	☐	☐
Issuing a tokenised financial instrument in compliance with national law	☐	☐	☐	☒	☐	☐
Transferring ownership (acquisitions, dispositions, earmarking etc) over a token, including good faith acquisition / bona fide ownership	☐	☐	☐	☐	☒	☐
Recognising ownership in a token towards third-parties	☐	☐	☐	☒	☐	☐
Using tokens as collateral	☐	☐	☐	☐	☒	☐
Possibility to differentiate between native and non-native tokens in national law	☐	☐	☐	☒	☐	☐
Recognising tokens as objects of property	☐	☐	☐	☒	☐	☐
Rights of token holders in intermediated custody chains	☐	☐	☐	☒	☐	☐
Enforcement and exercise of rights arising from/over tokens or the underlying assets	☐	☐	☐	☒	☐	☐
Custody of tokens	☐	☐	☐	☐	☒	☐
Treatment of tokens in insolvency proceedings including intermediary risk	☐	☐	☐	☐	☒	☐
Others	☐	☐	☐	☐	☐	☒

Please specify to what other issue(s) you refer in your answer to question 80.1:

The most significant issues are those that determine whether the holder of a token has an enforceable legal position against the issuer, intermediaries, third parties or an insolvency estate.

Particular importance should be attached to the transfer of ownership or entitlement, good-faith acquisition, third-party effects, custody chains and insolvency protection. These matters are essential where tokens are held through intermediaries or used within regulated financial structures.

For tokenised financial instruments and tokenised fund interests, the private-law treatment must remain compatible with existing sectoral requirements. These include safekeeping, asset segregation, investor rights, the enforceability of claims or rights represented by the token and the applicable rules on custody

and administration.

Native and non-native tokens should not be treated identically. Native tokens mainly raise questions of attribution, control, transfer and proprietary recognition. Non-native tokens require additional clarification because the token and the underlying legal position may diverge. Where a token represents an off-chain right or asset, the legal framework should ensure that a transfer of the token corresponds to the intended legal effect in respect of the represented right or asset.

The FMA considers that further clarification is required regarding the legal effects of Article 36(2) MiCA.

In particular, it is currently unclear whether Article 36(2) MiCA merely imposes an obligation on issuers to structure the reserve of assets in a manner that ensures protection in the event of insolvency, or whether MiCA itself is intended to confer insolvency protection on the reserve assets as a matter of EU law.

This distinction is important because the legal mechanisms available to achieve insolvency remoteness differ significantly across Member States. In practice, issuers may need to rely on national legal arrangements, such as trust structures, pledges, security interests or similar mechanisms, in order to ensure that reserve assets are protected from claims by creditors other than token holders in the event of insolvency.

The FMA further notes that clarification is also required regarding Article 37(1)(a) MiCA. It is currently unclear to what extent reserve assets may be subject to security arrangements that are established exclusively for the benefit of token holders and with the objective of enhancing insolvency protection.

For example, uncertainty exists as to whether reserve assets may be transferred to, or held through, a trust-like arrangement, or be subject to a pledge or comparable security interest in favour of token holders, where the sole purpose of such arrangement is to ensure that reserve assets remain protected from claims by other creditors in the insolvency of the issuer.

Greater clarity on these issues would improve legal certainty, facilitate consistent implementation across Member States and reduce the risk of divergent interpretations regarding the insolvency treatment of reserve assets under MiCA.

Please explain your answers to question 80.1 and provide examples from national law. In particular specify if any of the answers is specifically referring to native or non-native tokens and specify if any of the answers would be different depending on if the token is recording a tokenised financial instrument or crypto-assets:

No the answer is referring to stablecoins.

Question 80.2 What is the urgency with which each issue should be addressed by regulators?

	1 (none or not urgent)	2 (low urgency)	3 (moderate urgency)	4 (high urgency)	5 (immediate / critical)	Don't know No opinion Not applicable
Issuing a crypto-asset token in compliance with national law	☐	☐	☒	☐	☐	☐
Issuing a tokenised financial instrument in compliance with national law	☐	☐	☒	☐	☐	☐
Transferring ownership (acquisitions, dispositions, earmarking etc) over a token, including good faith acquisition / bona fide ownership	☐	☐	☒	☐	☐	☐
Recognising ownership in a token towards third-parties	☐	☐	☐	☒	☐	☐
Using tokens as collateral	☐	☐	☐	☒	☐	☐
Possibility to differentiate between native and non-native tokens in national law	☐	☒	☐	☐	☐	☐
Recognising tokens as objects of property	☐	☐	☒	☐	☐	☐
Rights of token holders in intermediated custody chains	☐	☐	☒	☐	☐	☐
Enforcement and exercise of rights arising from/over tokens or the underlying assets	☐	☐	☒	☐	☐	☐
Custody of tokens	☐	☐	☒	☐	☐	☐
Treatment of tokens in insolvency proceedings including intermediary risk	☐	☐	☐	☐	☒	☐
Others	☐	☐	☐	☐	☐	☒

Please specify to what other issue(s) you refer in your answer to question 80.2:

Please explain your answers to question 80.2 and provide examples from national law. In particular specify if any of the answers is specifically referring to native or non-native tokens and specify if any of the answers would be different depending on if the token is recording a tokenised financial instrument or crypto-assets:

Please explain your answer to question 80:

Yes, at least to some extent. Austrian private law contains general concepts that may be relevant for the assessment of tokens, in particular property-law, securities-law and custody-law concepts. However, there is currently no comprehensive statutory regime specifically addressing the private-law treatment of issuance, holding, transfer, custody, collateralisation and insolvency treatment of tokens.

MiCA and MiFID clarify the regulatory classification of certain assets and services, but they do not determine the proprietary nature of tokens, the transfer of ownership or entitlement, good-faith acquisition, third-party effects or the consequences of holding tokens through intermediaries. These matters remain primarily subject to national private law.

A differentiated approach appears necessary. Tokens representing rights raise different questions from tokens that do not represent rights (such as cryptocurrencies or certain non-fungible tokens). For rights-based tokens, the relationship between the token and the represented right should be clear. For tokens not representing rights, the relevant question is whether they can be attributed to a holder and transferred with sufficient legal certainty.

For regulated entities, these issues are particularly relevant where tokens are to be held, safeguarded, administered or transferred within regulated structures. Legal certainty regarding ownership or entitlement, transfer, custody, segregation, collateralisation and insolvency treatment is necessary to assess whether such assets can be appropriately held and whether investor or client rights can be effectively protected.

Question 81. Would you recommend increasing the legal certainty in the treatment of tokens through EU law?

☒ Yes

☐ No

☐ Don't know / no opinion / not applicable

Question 81.1. What are the 3 most important elements that should be addressed in EU law? Please explain your answer and provide examples:

Most important element number 1:

Most important element number 2:

Most important element number 3:

Question 81.2. Can legal certainty (ownership or entitlement, transfer and enforceability of rights recorded as tokens) be achieved under EU law in one of the following manners?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know No opinion Not applicable
Implementation of a 28th regime recognising legal effects of DLT registers holding tokens, including good-faith acquisition rules and rules on opposability/enforceability to third parties (erga omnes effects)	☐	☐	☐	☐	☐	☐
Full harmonisation of private law treatment of tokens in Member States	☐	☐	☐	☐	☐	☐
Partial harmonisation of private law treatment of tokens in Member States	☐	☐	☐	☒	☐	☐
Introducing a conflict of law regime for tokens under EU law	☐	☐	☐	☒	☐	☐
Other model	☐	☐	☐	☐	☐	☐

Please specify to what other measure(s) you refer in your answer to question 81.2:

Partial harmonisation combined with a functional clarification of selected legal effects appears preferable. Full harmonisation of Member States' private law would be difficult and may create unnecessary conflicts with national property-law systems.

A functional framework could define the legal effects of entries in qualifying DLT registers without replacing national property law. It could clarify attribution, transfer, third-party effects, enforceability, collateral use and protection against competing claims, provided that the relevant register meets minimum standards of uniqueness, reliable control, integrity, availability and minimum publicity.

A conflict-of-laws regime should also be considered. For intermediated holdings, the law of the relevant account or intermediary may provide a workable connecting factor. For decentralised or non-intermediated systems, a more tailored solution may be required because such systems may not have a clear territorial connection.

Please explain your answers to question 81.2 and provide examples, in particular from national law. Where you favour full or partial harmonisation or the introduction of a conflict of laws regime, please specify which legal instrument would be most appropriate for that purpose (a new Regulation or the use of existing regimes, such as MiFID or MiCA). Also consider if there are risks with establishing an ownership regime at EU level and how these risks could be mitigated:

Please explain your answer to question 81:

Yes, but only in a targeted and proportionate manner. It may be useful to consider EU-level clarification of selected private-law effects of tokens, in particular where cross-border holdings, custody chains or DLT-based transfers are involved.

A comprehensive harmonisation of Member States' private law does not appear necessary at this stage and could create frictions with established national property-law systems. A more proportionate approach would be to examine partial or functional clarification of specific legal effects, such as attribution,

transfer, enforceability, third-party effects, custody, segregation and insolvency treatment.

Such clarification should not create a parallel regime for tokenised financial instruments or tokenised fund interests. These instruments should remain subject to the applicable sectoral frameworks, including MiFID, AIFMD, UCITS and national fund law. The legal treatment should remain technology-neutral and should be determined by the legal and economic function of the token rather than by the use of DLT alone.

Question 82. There are different “ownership models” that could be used to increase legal certainty over tokens.

Please indicate maximum two models listed below that you think EU law could apply if it were to improve the legal certainty of tokens in the EU:

Maximum 2 selection(s)

- ☐ **MODEL 1:** The token is the asset by law, the law recognises a ledger-based asset and the ownership rights are constituted directly by the ledger entry.
 - ☒ **MODEL 2:** The token is the asset by law, where the law recognises that e.g. securities (dematerialised or physical) can be replaced by an entry into a DLT register and by this “replacing” (immobilisation) of the securities the function of the initial security is substituted by entry into a DLT register and the ownership rights are constituted by the representation on the ledger.
 - ☒ **MODEL 3:** Token is the asset by law. In this case the law does not actively regulate legal aspects such as what property is or how transfer of ownership occurs etc. but instructs on the legal consequences of entries in a DLT register (this is often called a functional approach). The law could at EU level stipulate who may exercise rights, i.e. the person recorded in the DLT register as holder of a tokenised asset, that these rights have full third-party effect and protects from competing claims. This also creates legal certainty for collateral use. The EU law would create a uniform rule of “digital entitlement” that functions across all Member States’ property law structures.
 - ☐ **MODEL 4:** The token is the legal carrier of rights associated with a related (often off-chain) asset. The law defines tokens as legal objects that do not create new rights, but can –like a “container” –represent various kinds of rights, such as membership rights, ownership, intellectual property rights, usage rights or rights of lien etc. The token would represent the rights stemming from the underlying assets and the law would ensure that the transfer of a token on the ledger legally transfers ownership of the rights stemming from the underlying asset.
- ([Inspired by Lichtenstein Law](#). Art 2 TVTG defines token as a piece of information on a TT System which can represent claims or rights of memberships against a person, rights to property, or other absolute or relative rights.
- Art 5 TVTG states that the TT Key holder has the power of disposal over the Token. It is further assumed that the person possessing the power of disposal over a Token also has the right to dispose of the Token. For every previous holder of the power of disposal, it is presumed that he was the person possessing the right of disposal at the time of this ownership).
- ☐ **MODEL 5:** Any other legal ownership structures, for example based on the approaches taken by different countries, including France, Germany, Luxembourg or adopted in other jurisdictions or internationally, that could be implemented in EU law.

You selected:

MODEL 1: The token is the asset by law, the law recognises a ledger-based asset and the ownership rights are constituted directly by the ledger entry.

MODEL 1 - a) What would be the legal interoperability of any such EU level measure with national private laws of Member States, or at least laws of the Member State that you are familiar with?

MODEL 1 - b) Is it preferable to establish constitutive rules of ownership based on the asset being recorded on chain or functional rules regulating the effects of recording an asset on chain?

- ☐ Constitutive rules of ownership based on the asset being recorded on chain
- ☐ Functional rules regulating the effects of recording an asset on chain
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 1 b):

MODEL 1 - c) Are the different ownership models better suited for native or non-native tokens?

- ☐ For native
- ☐ For non-native tokens
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 1 c):

MODEL 1 - d) Can the same ownership model be implemented for all types of tokens (crypto-assets and DLT financial instruments)?

- ☐ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

MODEL 1 - d) What would need to be different depending on the type of the token?

Please explain your answers for MODEL 1 and provide examples:

You selected:

MODEL 2: The token is the asset by law, where the law recognises that e.g. securities (dematerialised or physical) can be replaced by an entry into a DLT register and by this “replacing” (immobilisation) of the securities the function of the initial security is substituted by entry into a DLT register and the ownership rights are constituted by the representation on the ledger.

MODEL 2 - a) What would be the legal interoperability of any such EU level measure with national private laws of Member States, or at least laws of the Member State that you are familiar with?

Model 2 appears broadly compatible with Austrian private law where the token or register entry replaces the function of a traditional security or fund unit. It allows the legal effects of a traditional instrument to be maintained while the medium of representation changes. This appears particularly suitable for tokenised financial instruments and fund interests, provided that existing sectoral requirements remain applicable.

MODEL 2 - b) Is it preferable to establish constitutive rules of ownership based on the asset being recorded on chain or functional rules regulating the effects of recording an asset on chain?

- ☐ Constitutive rules of ownership based on the asset being recorded on chain
- ☒ Functional rules regulating the effects of recording an asset on chain
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 2 b):

Functional rules appear preferable. They can determine the legal consequences of a register entry without fully replacing national property-law concepts. This allows legal certainty for issuance, holding, transfer and custody while preserving compatibility with existing securities, fund and custody law.

MODEL 2 - c) Are the different ownership models better suited for native or non-native tokens?

- ☐ For native
- ☐ For non-native tokens
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 2 c):

MODEL 2 - d) Can the same ownership model be implemented for all types of tokens (crypto-assets and DLT financial instruments)?

- ☐ Yes
- ☒ No

☐ Don't know / no opinion / not applicable

MODEL 2 - d) What would need to be different depending on the type of the token?

The same model should not apply to all types of tokens. For tokenised financial instruments and fund interests, the model must preserve the application of sectoral law. For crypto-assets that do not represent rights, the focus should be on attribution, control and transfer of the token itself. For tokens representing off-chain assets, additional rules are needed to ensure alignment between the ledger entry and the underlying legal position.

Please explain your answers for MODEL 2 and provide examples:

--

You selected:

MODEL 3: Token is the asset by law. In this case the law does not actively regulate legal aspects such as what property is or how transfer of ownership occurs etc but instructs on the legal consequences of entries in a DLT register (this is often called a functional approach). The law could at EU level stipulate who may exercise rights, i.e. the person recorded in the DLT register as holder of a tokenised asset, that these rights have full third-party effect and protects from competing claims. This also creates legal certainty for collateral use. The EU law would create a uniform rule of “digital entitlement” that functions across all Member States’ property law structures.

MODEL 3 - a) What would be the legal interoperability of any such EU level measure with national private laws of Member States, or at least laws of the Member State that you are familiar with?

Model 3 appears compatible with different national private-law systems because it focuses on the legal effects of register entries rather than on harmonising ownership concepts. It could provide a common layer of legal certainty by defining entitlement, transfer effects, third-party protection and enforceability, while leaving the underlying property-law structure to Member States.

MODEL 3 - b) Is it preferable to establish constitutive rules of ownership based on the asset being recorded on chain or functional rules regulating the effects of recording an asset on chain?

- ☐ Constitutive rules of ownership based on the asset being recorded on chain
- ☒ Functional rules regulating the effects of recording an asset on chain
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 3 b):

Functional rules are preferable. They allow EU law to define specific effects of DLT register entries, such as entitlement and enforceability, without establishing a comprehensive EU ownership regime. This reduces the risk of conflicts with national private law.

MODEL 3 - c) Are the different ownership models better suited for native or non-native tokens?

- ☐ For native
- ☐ For non-native tokens
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 3 c):

MODEL 3 - d) Can the same ownership model be implemented for all types of tokens (crypto-assets and DLT financial instruments)?

☐ Yes

☒ No

☐ Don't know / no opinion / not applicable

MODEL 3 - d) What would need to be different depending on the type of the token?

For native tokens, rules on attribution, control and transfer may be sufficient. For tokenised financial instruments and fund interests, the model must respect sectoral law. For non-native tokens, the legal link between the token and the underlying right or asset must be clarified separately.

Please explain your answers for MODEL 3 and provide examples:

You selected:

MODEL 4: The token is the legal carrier of rights associated with a related (often off-chain) asset. The law defines tokens as legal objects that do not create new rights, but can –like a “container” –represent various kinds of rights, such as membership rights, ownership, intellectual property rights, usage rights or rights of lien etc. The token would represent the rights stemming from the underlying assets and the law would ensure that the transfer of a token on the ledger legally transfers ownership of the rights stemming from the underlying asset.

MODEL 4 - a) What would be the legal interoperability of any such EU level measure with national private laws of Member States, or at least laws of the Member State that you are familiar with?

MODEL 4 - b) Is it preferable to establish constitutive rules of ownership based on the asset being recorded on chain or functional rules regulating the effects of recording an asset on chain?

- ☐ Constitutive rules of ownership based on the asset being recorded on chain
- ☐ Functional rules regulating the effects of recording an asset on chain
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 4 b):

MODEL 4 - c) Are the different ownership models better suited for native or non-native tokens?

- ☐ For native
- ☐ For non-native tokens
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 4 c):

MODEL 4 - d) Can the same ownership model be implemented for all types of tokens (crypto-assets and DLT financial instruments)?

- ☐ Yes
- ☐ No

☐ Don't know / no opinion / not applicable

MODEL 4 - d) What would need to be different depending on the type of the token?

Please explain your answers for MODEL 4 and provide examples:

You selected:

MODEL 5: Any other legal ownership structures, for example based on the approaches taken by different countries, including France, Germany, Luxembourg or adopted in other jurisdictions or internationally, that could be implemented in EU law.

MODEL 5 - a) What would be the legal interoperability of any such EU level measure with national private laws of Member States, or at least laws of the Member State that you are familiar with?

MODEL 5 - b) Is it preferable to establish constitutive rules of ownership based on the asset being recorded on chain or functional rules regulating the effects of recording an asset on chain?

- ☐ Constitutive rules of ownership based on the asset being recorded on chain
- ☐ Functional rules regulating the effects of recording an asset on chain
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 5 b):

MODEL 5 - c) Are the different ownership models better suited for native or non-native tokens?

- ☐ For native
- ☐ For non-native tokens
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 5 c):

MODEL 5 - d) Can the same ownership model be implemented for all types of tokens (crypto-assets and DLT financial instruments)?

- ☐ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

MODEL 5 - d) What would need to be different depending on the type of the token?

Please explain your answers for MODEL 5 and provide examples:

Question 83. Comparing national laws of Member States, what are the main differences in how national laws governs the issuance, holdings and transfers of tokens? Please explain your answer and provide examples:

National laws differ significantly in whether and how they recognise tokens as objects capable of proprietary attribution, transfer and third-party protection. Some jurisdictions have introduced specific regimes for electronic securities, register-based rights or tokenised assets. Others rely mainly on general property, contract, securities and custody law.

These differences affect whether a token holder is treated as owner, creditor, co-owner, beneficiary or merely as holder of a contractual claim. They also affect whether a transfer on a DLT register has third-party effect, whether good-faith acquisition is possible, whether tokens can be pledged, and whether client assets are protected in the insolvency of an intermediary.

In Austria, there is not yet a comprehensive statutory private-law regime for all tokenised assets. While certain digital or dematerialised securities structures exist, broader questions concerning proprietary attribution, transfer, good-faith acquisition, custody and insolvency treatment of tokens are not comprehensively codified.

These differences are particularly relevant in cross-border settings, where the DLT system, issuer, intermediary and investor may be located in different jurisdictions. A targeted EU framework could therefore be useful, provided it focuses on minimum legal effects, interoperability, custody, segregation, insolvency treatment and conflict-of-laws rules, while respecting national private-law structures.

4.7 Questions on conflicts of law

Financial Collateral Directive (FCD) and Settlement Finality Directive (SFD) entails targeted conflict of law rules, mainly applicable to financial instruments hence broadly relevant for DLT financial instruments, however the current regime leaves a potential gap where the token does not qualify under the scope of FCD and SFD or where existing conflict rules do not easily lend its application to tokens. As noted in the [UNIDROIT Principles on digital assets and private law](#) the usual connecting factors for choice-of-law rules, such as the location of persons, offices, activity, or assets have less of a useful role for DLT financial instruments and crypto-assets and the approach would rather be to identify connecting factors relevant to such instruments and assets.

Question 84. Should EU law introduce a conflict of law rule for tokens?

- ☐ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Question 84.1 please explain why the current conflict of law rules applicable in EU are not enough or sufficiently clear in its application to tokens?

Question 84.2. If the EU would introduce conflict of law rules for proprietary aspects of tokens, what would be the preferred connecting factors? Rank the below listed connection factors from 1 to 5 (1 being the most relevant connecting factor and 5 the least relevant connection factor).

Connecting factors without a ranking will be considered not relevant:

at most 5 answered row(s)

	1	2	3	4	5
The law of the state specified in the token or in the principles (if any) expressly specified in the token	☐	☐	☐	☐	☐
The law of the state specified in the rules or in the principles of the system on which the token is recorded	☐	☐	☐	☐	☐
The law of the state in which the legal entity operating the DLT-based system on which tokens are recorded	☐	☐	☐	☐	☐
In relation to a token for which there is an issuer, the law of the state where the issuer is established	☐	☐	☐	☐	☐
In relation to tokens for which there is an issuer, the law of the state under whose supervision the issuer operates	☐	☐	☐	☐	☐
In relation to tokens for which there is a provider of the technologies creating or issuing the tokens, the law of the state under whose supervision such technology operates	☐	☐	☐	☐	☐
Where a token shall be registered, the law of the state under whose supervision the register is maintained	☐	☐	☐	☐	☐
The law of the state of the relevant operating authority/administrator (PROPA), meaning a state authority or a body (e.g., a foundation) that takes over the administration of the system onto which the token is registered	☐	☐	☐	☐	☐
The law of the state of the primary residence of the encryption private master keyholder (PREMA), meaning the seat of a body that holds a system-relevant master key, with the help of which coercive transactions can be carried out, for example, based on a court order	☐	☐	☐	☐	☐
Any other?	☐	☐	☐	☐	☐

Please specify to what other factor(s) you refer in your answer to question 84.2:

Please explain your answers to question 84, 84.1 and 84.2 and provide examples.

In answering this question, please consider if the suggested scope of the conflict of law rule in your view is the right one, and whether there are aspects missing:

Please explain your answer to question 84:

Question 85. If there are any other issues relating to legal certainty which are not mentioned above, please describe them here:

Unauthorized Global Stablecoins and Enforcement Challenges

The FMA considers that the treatment of large third-country stablecoin issuers operating outside the MiCA framework deserves further attention.

Practical experience since the application of MiCA suggests that the existing framework may not provide competent authorities with sufficiently effective tools to address situations where a large stablecoin issuer deliberately remains outside the EU authorisation framework while continuing to achieve significant circulation and usage within the Union.

In this context, the recent clarification by the European Commission in ESMA Q&A No. 2404 is particularly relevant. The Commission clarified that not every form of distribution of a non-authorised stablecoin is prohibited under MiCA. While public offers and admissions to trading of ARTs and EMTs without a MiCA-compliant issuer are restricted, other activities that may facilitate access to or use of such stablecoins do not necessarily fall within the current prohibition framework.

As a result, a stablecoin may achieve significant adoption within the Union despite the absence of a MiCA authorisation, while neither the issuer nor the relevant CASPs clearly fall within the existing provisions governing issuers, public offers, or other forms of market distribution.

The FMA therefore considers that the European Commission should assess whether MiCA provides competent authorities with sufficient powers to address the circulation, distribution and use of unauthorised stablecoins within the Union, particularly where such stablecoins reach significant scale or become systemically relevant.

In the context of a future review of MiCA ("MiCA 2.0"), the EU legislator should consider whether distribution-related activities beyond the concept of a

public offer should be subject to additional restrictions where they effectively promote market adoption and usage of non-compliant stablecoins within the Union. Competent authorities should be provided with clear and harmonised intervention powers to address such situations.

Failure to address these issues may create incentives for regulatory arbitrage and place authorised MiCA-compliant issuers at a competitive disadvantage compared to global stablecoin issuers that choose not to seek authorisation within the Union while nevertheless benefiting from access to EU users through secondary market trading and cross-border distribution channels.

From a supervisory perspective, one possible solution could be the introduction of a harmonised framework requiring CASPs to delist stablecoins that have been identified as non-compliant with the MiCA framework. To ensure consistency across Member States, EBA could be empowered to maintain a central EU register of stablecoins assessed as non-compliant, with NCAs being responsible for the enforcement of the corresponding obligations at national level.

4.8 Final open question

Question 86. Interested parties that wish to bring other relevant issues, not raised in this consultation, to the Commission's attention, should feel free to communicate them here:

Authorisation exemption for ART issuers under Art 16 No 2 MiCAR

The FMA considers the exemptions under Article 16 (2) MiCA to be difficult to supervise and recommends reassessing them.

The exemption for offers addressed solely to qualified investors (Art. 16 (2)) is particularly challenging. Market participants have explored structures relying on this exemption even where it is unclear whether access is genuinely restricted to qualified investors. Given the transferable nature of crypto-assets, enforcing such restrictions is difficult. Further clarification is needed on the definition of a qualified investor and on safeguards preventing circumvention of the ART authorisation regime.

The EUR 5 million threshold exemption (Art. 16 (2) (a)) also raises concerns. Without dedicated reporting requirements, competent authorities face difficulties in verifying compliance. Visibility is limited where tokens are traded across multiple venues, transferred through self-hosted wallets or held outside regulated intermediaries.

More generally, exempt issuers must notify a crypto-asset white paper to competent authorities, but MiCA does not clearly define the purpose of this notification, the expected supervisory review or the powers available where exemptions are misapplied.

The European Commission should therefore assess whether these exemptions remain necessary and proportionate. Narrowing or removing them could enhance legal certainty, supervisory consistency and a more uniform regulatory framework for ART issuances across the EU.

Article 38 MiCA – Uncertainty Regarding the Concept of “Investment of the Reserve of Assets”

The FMA considers that further clarification is required regarding the scope and application of Article 38(1) MiCA.

In practice, it remains unclear what constitutes an "investment" of reserve assets for the purposes of Article 38 and under which circumstances the requirements relating to highly liquid financial instruments (HLFIs) become applicable.

This issue has arisen in particular in the context of commodity-linked ART projects. For example, the FMA assessed a proposed gold-linked token intended to maintain a stable value by reference to the price of physical gold traded on the London Bullion Market. To achieve this objective, the issuer intended to hold physical gold as part of the reserve of assets.

In this context, uncertainty arose as to whether the holding of physical gold in the reserve of assets constitutes an investment within the meaning of Article 38(1) MiCA and therefore triggers the requirement that reserve assets be invested only in HLFIs with minimal market, credit and concentration risk.

During discussions with the EBA, the understanding emerged that Article 38(1) may not apply where there is no change in the nature of the referenced assets. Under this interpretation, if an issuer receives physical gold and directly holds that gold in the reserve of assets, Article 38(1) would not be triggered. By contrast, if the issuer receives cash and subsequently uses that cash to purchase physical gold for inclusion in the reserve, this could constitute an investment for the purposes of Article 38(1), with the consequence that the HLI requirements would apply and physical gold could not be part of the reserves.

The FMA considers that this distinction is not apparent from the wording of the current Level 1 text and creates considerable legal uncertainty. In addition, certain elements of the Level 2 framework appear difficult to reconcile with this interpretation, further increasing uncertainty for issuers and supervisors.

Clarification is therefore required as to:

- when an "investment" within the meaning of Article 38(1) MiCA occurs;
- under which circumstances the HLI requirements become applicable;
- whether the assessment depends on the original form in which reserve assets are received by the issuer; and
- how Article 38 should apply to commodity-linked ARTs whose value is intended to track the value of specific reference assets such as gold.

The FMA notes that the current uncertainty may significantly restrict the practical viability of certain ART structures. In particular, commodity-linked ARTs may become difficult or impossible to structure where the issuer is required to hold reserve assets exclusively in HLFIs despite the token being designed to reference a commodity.

The European Commission should therefore clarify the intended interaction between Articles 36 and 38 MiCA at Level 1 and provide greater certainty regarding the treatment of commodity-backed reserve assets. Such clarification would promote consistent supervisory outcomes and facilitate the development of viable ART business models in line with the objectives of MiCA.

Extension of Public Warnings to Unauthorised Activities

The FMA welcomes the framework for public warnings provided under Article 94(1)(e) MiCAR, which allows competent authorities to issue public warnings where a crypto-asset service provider fails to comply with its obligations under the MiCAR. However, investor protection concerns are not limited to infringements committed by authorised entities, but also arise where crypto-asset services are provided without the required authorisation altogether and also cases where no crypto-asset service is formally offered while communications, marketing practices, or other circumstances create the impression that a regulated crypto-asset service is being provided. The FMA therefore considers it essential that the warning power is explicitly extended to cases of unauthorised business activity and such cases in which the impression is given. Public warnings regarding unauthorised entities would enhance

transparency, help investors identify entities operating outside the regulatory perimeter, and strengthen deterrence against unlawful market conduct. Such an extension would close an important supervisory gap and further support the objectives of investor protection and market integrity under MiCAR. To strengthen the single market, regulatory approaches should be harmonized not only with regard to the sanctioning of unauthorized service providers but also with regard to related public warnings.

Investor Compensation Schemes

The FMA notes that, unlike clients of investment firms under the MiFID II framework, clients of Crypto-Asset Service Providers are generally not covered by a harmonised investor-compensation scheme. As a result, clients may be exposed to significant losses where a CASP is unable to return client assets or fulfil its obligations and existing liability, segregation, or insolvency safeguards prove insufficient. While increased prudential requirements and especially higher minimum capital requirements can strengthen the resilience of CASPs (see also the answer to Question 50), they cannot provide the same level of protection as an investor-compensation scheme. The FMA therefore considers it appropriate to assess whether a compensation framework comparable to that applicable under the MiFID II should be introduced for CASPs. Such a framework would enhance investor protection, strengthen confidence in the crypto-asset market, and contribute to a more consistent regulatory treatment of functionally comparable investment activities. The issue of investor compensation should be considered in conjunction with the question of adequate capital adequacy.

Audit Requirements for Annual Financial Statements

The FMA considers the introduction of harmonised accounting and statutory audit requirements for Crypto-Asset Service Providers and non-credit-institution Asset-Referenced Token issuers to be essential for effective supervision. In contrast to investment firms operating under the MiFID II framework, which are subject to established accounting, reporting and audit requirements, MiCAR currently does not provide a comparable framework which would work for CASPs as well as non-credit-institution ART issuers. For entities covered by Article 60 MiCAR, in particular, this means that they are subject to the requirements of MiFID II for their investment services, but not for their crypto-asset services. This distinction, in turn, creates such a significant administrative burden that entities covered by Article 60 MiCAR either comply with the requirements incompletely or excessively, or spin off one group of services into a subsidiary. The absence of standardised and audited annual financial statements creates significant supervisory risks and limits the comparability of financial information across entities. Standardised and audited financial statements are a prerequisite for data-driven and risk-based supervision, enabling competent authorities to assess the financial soundness and business models of supervised institutions on a consistent basis.