|  |
| --- |
| Reply form to the Consultation Paper on certain requirements of the Markets in Crypto Assets Regulation (MiCA) on detection and prevention of market abuse, investor protection and operational resilience – third consultation paper |
|  |

**Responding to this paper**

ESMA invites comments on all matters in this consultation paper and in particular on the specific questions. Comments are most helpful if they:

* respond to the question stated;
* indicate the specific question to which the comment relates;
* contain a clear rationale; and
* describe any alternatives ESMA should consider.

ESMA will consider all comments received by **25 June 2024.**

**Instructions**

In order to facilitate analysis of responses to the Consultation Paper, respondents are requested to follow the below steps when preparing and submitting their response:

1. Insert your responses to the questions in the Consultation Paper in the present response form.
2. Use this form and send your responses in Word format (**pdf documents will not be considered except for annexes**);
3. Please do not remove tags of the type <ESMA\_QUESTION \_MIC4\_1>. Your response to each question has to be framed by the two tags corresponding to the question.
4. If you do not wish to respond to a given question, please do not delete it but simply leave the text “TYPE YOUR TEXT HERE” between the tags.
5. When you have drafted your response, name your response form according to the following convention: ESMA\_MIC4\_nameofrespondent\_RESPONSEFORM. For example, for a respondent named ABCD, the response form would be entitled ESMA\_MIC4\_ABCD\_RESPONSEFORM.
6. Upload the form containing your responses, **in Word format**, to ESMA’s website (www.esma.europa.eu under the heading “Your input – Open Consultations” -> Consultation Paper on guidelines on conditions and criteria for the classification of crypto-assets as financial instruments”).

**Publication of responses**

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publically disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA’s rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESMA’s Board of Appeal and the European Ombudsman.

**Data protection**

Information on data protection can be found at [www.esma.europa.eu](http://www.esma.europa.eu) under the heading [Legal Notice](http://www.esma.europa.eu/legal-notice).

**Who should read this paper**

# All interested stakeholders are invited to respond to this consultation paper. In particular, ESMA invites crypto-assets issuers, crypto-asset service providers and financial entities dealing with crypto-assets as well as all stakeholders that have an interest in crypto-assets.

**General information about respondent**

|  |  |
| --- | --- |
| Name of the company / organisation | Juscutum |
| Activity | Audit/Legal/Individual |
| Are you representing an association? |[x]
| Country/Region | Other |

**Questions**

1. Do you agree with ESMA’s analysis on the personal scope of Article 92 of MiCA? Are there other types of entities in the crypto-asset markets that should be considered as a PPAET (e.g. miners/validators)? Do you believe that CASPs providing custody and administration of crypto-assets on behalf of clients should also be considered as PPAETs for the purpose of this RTS? Please elaborate.

<ESMA\_QUESTION\_MIC4\_1>

We agree that CASPs providing custody and administration of crypto-assets on behalf of clients should also be considered as PPAETs for this RTS. CASPs should prevent market abuse while abusers try to use their services.

On the other hand, we suppose that some types of entities in crypto-asset markets that do not store customers' funds or do not deal with customers' behaviour (e.g., miners, validators, traders of their assets) should not fall under the scope of Article 92.

<ESMA\_QUESTION\_MIC4\_1>

1. Do you agree with the proposed elements that should constitute appropriate arrangements, systems and procedures to detect and prevent market abuse? If not, please specify the article of the draft RTS and elaborate.

<ESMA\_QUESTION\_MIC4\_2>

We agree with the proposed elements in general. We recommend adding specific timelines to Articles 4 (Training) and 5 (Reporting obligations) to ensure clarity.

For instance, Article 4 could mandate staff training at least once annually. Similarly, Article 5 could require submission of the STOR immediately but no later than 48 hours after the relevant obligation arises.

<ESMA\_QUESTION\_MIC4\_2>

1. Do you agree with the proposed STOR template as presented in the Annex of the RTS?

<ESMA\_QUESTION\_MIC4\_3>

We agree with the STOR template provided in the Annex.

<ESMA\_QUESTION\_MIC4\_3>

1. Is there any parameter or naming convention that in your view should be modified to facilitate the identification of suspicious orders/transactions/behaviours involving crypto-assets?

<ESMA\_QUESTION\_MIC4\_4>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_4>

1. In Section II of the Annex, would the concept of ‘location’ be applicable to a distributed ledger? For instance, would the IP address of miners/validator nodes in the network be useful in a context where it can be masked through VPNs?

<ESMA\_QUESTION\_MIC4\_5>

It is possible to ask for a location for such usage. At the same time, using VPNs could hide IP addresses. Distributed ledgers cannot always prove the address if customers try to mask their IP. That is why, from a practical approach, the usage is limited.

<ESMA\_QUESTION\_MIC4\_5>

1. Is there any other element or information relevant to crypto-asset markets that in your view should be included in the template? Please explain.

<ESMA\_QUESTION\_MIC4\_6>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_6>

1. Please provide information about the estimated costs and benefits of the proposed technical standard, in particular in relation to the arrangements, systems and procedures to prevent and detect market abuse.

<ESMA\_QUESTION\_MIC4\_7>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_7>

1. Do you agree with ESMA’s approach regarding consistency between the MiCA and MiFID II suitability regimes? If you think that the two regimes should diverge, where and for which reasons?

<ESMA\_QUESTION\_MIC4\_8>

We advocate for a complementary regulatory approach that leverages both MiFID II and MiCA for crypto-assets. This would ensure a harmonised framework that effectively addresses the unique characteristics of securities and other crypto-assets. Specifically, we propose that:

Securities falling under MiFID II's definition should be subject to joint regulation by MiFID II and MiCA. This would ensure comprehensive oversight encompassing both traditional securities frameworks and the innovative elements introduced by MiCA.

Other crypto-assets not classified as securities under MiFID II should be primarily regulated under MiCA. This would avoid unnecessary duplication and allow MiCA's tailored approach to flourish.

<ESMA\_QUESTION\_MIC4\_8>

1. Do you think that the draft guidelines should be amended to better fit crypto-assets and the relevant crypto-asset services? In which regard? Please justify your answer.

<ESMA\_QUESTION\_MIC4\_9>

The draft guidelines are general. We recommend amending the guidelines with specific requirements and examples of proper implementation for CASPs. It would also be great to add the most common or possible mistakes and options for improvement.

<ESMA\_QUESTION\_MIC4\_9>

1. Do you agree with the approach followed by ESMA regarding periodic statements provided in relation to portfolio management of crypto-assets?

<ESMA\_QUESTION\_MIC4\_10>

We agree, in general, with the approach followed by ESMA regarding periodic statements provided about portfolio management of crypto-assets. We recommend providing guidance for portfolio managers with the proper form of statements and methods. Additionally, we recommend giving customers of portfolio managers the possibility to initiate changing the required terms from quarterly statements to suitable periods depending on their investment strategy. We recommend setting up monthly periodic statements for unqualified investors and 3-month periods for accredited investors as an essential term.

<ESMA\_QUESTION\_MIC4\_10>

1. Do you agree with the approach taken by ESMA in the draft guidelines for crypto-asset service providers providing transfer services for crypto-assets on behalf of clients as regards procedures and policies, including the rights of clients? Please also state the reasons for your answer.

<ESMA\_QUESTION\_MIC4\_11>

We agree with the approach; it covers all possible questions.

<ESMA\_QUESTION\_MIC4\_11>

1. Do you think that the draft guidelines address sufficiently the risks for clients related to on- and off-DLT crypto-asset transfers? Please justify your answer.

<ESMA\_QUESTION\_MIC4\_12>

We agree with the approach; it covers all possible questions.

<ESMA\_QUESTION\_MIC4\_12>

1. Are there any additional comments that you would like to raise and/or information that you would like to provide, for example, on whether other relevant points or clients’ rights should be considered?

<ESMA\_QUESTION\_MIC4\_13>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_13>

1. Do you support ESMA’s interpretation of the term, ‘systems’ in the mandate? If not, please explain your understanding of the term (and provide examples if possible).

<ESMA\_QUESTION\_MIC4\_14>

Systems:

* 1. Focus on technical aspects:

 This interpretation dives deeper into the technological components of a CASP's "systems." It would explore specific security protocols, data encryption, and access control mechanisms. This would be beneficial if you're interested in the technical nitty-gritty of how CASPs ensure security.

* 1. Focus on overall compliance:

 This interpretation emphasises the broader picture of how CASPs manage risk and adhere to regulations through their systems. It would delve into the governance and risk management procedures, like KYC/AML checks and trade monitoring systems. This would be useful if you're more interested in MiCA's regulatory framework and how CASPs comply with it.

<ESMA\_QUESTION\_MIC4\_14>

1. Are there other ‘appropriate Union standards’ beyond those identified in the consultation paper that you consider relevant for this mandate? If yes, please list them and provide a rationale for why they would be relevant.

<ESMA\_QUESTION\_MIC4\_15>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_15>

1. Do you agree with the inclusion of minimal administrative arrangements in Guideline 2 (i.e., no reference to implementing a risk management framework)? If no, please explain whether you would consider either *fewer* or *more* administrative arrangements appropriate.

<ESMA\_QUESTION\_MIC4\_16>

The current proposal to implement a DORA-compliant risk management framework might be overly burdensome for CASPs. The complexity and cost associated with such a framework could be excessive, particularly for smaller CASPs.

We recommend a tiered risk management framework that considers the size and operational complexity of CASPs. Large, established CASPs with significant custodial responsibilities (like Binance, OKX, and Coinbase) would likely require a more comprehensive DORA-aligned framework. ESMA should provide criteria for substantial responsibilities, including the level of responsibility for customers' funds.

A less complex, risk-based approach could be implemented for smaller CASPs. This approach could focus on essential controls that are aligned with MiCA's consumer protection and market integrity goals. Excluding CASPs that don't offer custodial services from the strictest requirements could be a sensible option.

<ESMA\_QUESTION\_MIC4\_16>

1. Do you support the inclusion of Guideline 5 on ‘cryptographic key management’? Do you consider cryptographic keys relevant as either a ‘system’ or a ‘security access protocol’? Is this guideline fit for purpose (i.e., can cryptographic keys be ‘replaced’ as implied in paragraph 29 of the draft guidelines)?

<ESMA\_QUESTION\_MIC4\_17>

While cryptographic keys are not systems but essential security components, we agree that ‘cryptographic key management’ is a system that helps to secure keys. So, they should be included in Guideline 5.

<ESMA\_QUESTION\_MIC4\_17>