|  |
| --- |
| 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 | Auditchain Labs AG |
| Activity | Audit/Legal/Individual |
| Are you representing an association? |  |
| Country/Region | Switzerland |

**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>

TYPE YOUR TEXT HERE

<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>

TYPE YOUR TEXT HERE

<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>

Auditchain Labs AG recommends that the STOR form itself should be provided in machine readable format using XBRL, using a taxonomy that is designed to be fully compatible, or even using the same model, that already being required for white papers. Using the same approach would make it easier for automated analysis, alerting, and detection of patterns and trends both for a given entity and across entities.

Several items of information requested, such as National Insurance Number are generally treated as sensitive and held to be Personal Information under GDPR. Assurance, such as appropriate masking or the use of privacy enhancing technologies (PETs), needs to be provided such that supplying NINs will not constitute a violation of GDPR. The same applies to other information requested about natural persons such as employment and address. Recordings of conversations (mentioned under “documentation attached”) should be disclosed and described, even though the circumstances of such records may be illegal.

We have the following detailed comments on the template:

**First line:** The wording should reflect that the reporter may not be a “person professionally arranging or executing transactions in crypto assets” and may be principally performing other roles. Moreover, the form should encourage any party – i.e., a “whistleblower” - who becomes aware of such activity to submit a STOR on the principle of “if you see something, say something”. Such an approach would maximize the safety of the market and protect client’s rights.

**Name of the reporting entity:** in the same way that a LEI is requested using an ISO code (ISO 17442), the legal form should be requested using ISO 20575 which is already made use of for LEI registration and has values publicly available <https://www.gleif.org/en/about-lei/code-lists/iso-20275-entity-legal-forms-code-list>

**Address of the reporting entity: The form should require description of whether the address** is the entity’s headquarters, registered legal address, the actual office of the reporter that is being requested, or any combination of the above. This distinction is already made in the external reporting taxonomies and a unified standard approach would be interoperable.

**Type of trading activity:** This submission should also indicate whether the suspicious activity is a regular activity of the reporting entity or solely that related to the suspicious activity (if any).

**Description of the distributed ledger:** This item is redundant if a Digital Token Identifier (DTI) is provided, as requested in the previous question.

**Description of the order:** Several of the characteristics requested may not be applicable depending on the nature of the suspicious activity (e.g., “Transactions designed to fail won’t have a settlement”).

Some of the fields related to order submission are unclear:  
- what information is expected for the “way” and “means” the order was placed;  
- it’s unlikely it will be a “person” receiving the order

**Address**: As per the comment above (“Address of the Reporting Entity”), there should be a requirement to identify whether the address is for an office, headquarters, or registered address of an entity. And for a natural person the home or business address as specified in the iXBRL taxonomy, as mentioned above.

**Additional information: It is** unclear what is meant by the term “trading desk” when most crypto asset activity is software-automated and not associated with a “desk” as in traditional financial activity.

**Documentation attached: The wording here is unclear:** Does “media comment” mean comment BY external media, or comment ON any media attached?

<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>

TYPE YOUR TEXT HERE

<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>

TYPE YOUR TEXT HERE

<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>

TYPE YOUR TEXT HERE

<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>

TYPE YOUR TEXT HERE

<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>

TYPE YOUR TEXT HERE

<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>

TYPE YOUR TEXT HERE

<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>

Persons professionally arranging or executing transactions in crypto-assets on behalf of clients interact with systems that publish quotes and execute orders. In 7.2.1 RTS on arrangements, systems and procedures for detecting and reporting suspected market abuse in crypto-assets, there are specifications that systems be maintained to detect market abuse but is not explicit about how this could be achieved. This gives the term “systems” a broad definition leaving no prescription for systemic prevention of abuse.

There are many “procedures” that can be programmed in order management systems that trigger actions if conditions are met. When client orders are entered, procedures to protect the rights of clients should also exist.

An example would be a systemic distinction between a client order and account and an order/account entered by and on behalf of persons professionally arranging or executing transactions on behalf of clients. Additionally, if a program existed within the same system where a person professionally arranging or executing transactions on behalf of clients bought 100 crypto-assets at €10 on its own behalf when holding client limit orders to buy at €10 equalling, in aggregate, 1000 crypto-assets, the person professionally arranging or executing transactions would be required to fill 100 crypto-assets of the client limit orders.

Such procedures would provide additional “systemic definition” that would protect clients’ rights. Additionally, in such cases where the client order was entered with the order entered by and on behalf of persons professionally arranging or executing transactions, the condition that protects the client would be triggered and an exception report might be captured. This type of report would provide statistics that can be used to measure the frequency and nature of the fiduciary performance of persons professionally arranging or executing transactions on behalf of clients.

Such events and exception reports could be captured and transmitted in XBRL for the purposes of interoperability with external reporting systems which may reduce the costs of compliance, enhance transparency, and provide important and durable investor protections.

<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>

TYPE YOUR TEXT HERE

<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>

TYPE YOUR TEXT HERE

<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>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_17>