25 March 2023
ESMA75-453128700-1002

Consultation Paper

Draft technical standards and guidelines specifying 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 paper and in particular on the specific questions summarised in Annex I. 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 **Tuesday, 25 June 2024.**

All contributions should be submitted online at www.esma.europa.eu under the heading 'Your input - Consultations'.

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 publicly 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 under the heading 'Data protection'.

Who should read this paper?

All interested stakeholders are invited to respond to this consultation paper. In particular, ESMA invites investors and their associations, crypto-asset issuers, crypto-asset service providers, offerors and persons seeking admission to trading of crypto-assets, financial entities dealing with crypto-assets and any other stakeholders that have an interest in the market for crypto-assets.

List of acronyms

AIF	Alternative investment fund
ART	Asset-referenced token
CASP	Crypto-asset service provider
DLT	Distributed ledger technology
EBA	European Banking Authority
EMT	Electronic money token
ESMA	European Securities and Markets Authority
ESAs	European Supervisory Authorities
ICT	Information and communications technology
ITS	Implementing technical standards
MAR	Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (MAR)
MiCA	Regulation (EU) 2023/1114 of the European Parliament and the Council of 31 May 2023 on markets in crypto-assets (MiCA)
MiFID II	Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MiFID II)
NCA	National competent authority
RTS	Regulatory technical standards
UCITS	Undertakings for collective investments in transferable securities

Table of Contents

1 Executive Summary

Reasons for publication

The Regulation on markets in crypto-assets (MiCA) was published in the Official Journal of the EU on 9 June 2023. The European Securities and Markets Authority (ESMA) has been empowered to develop technical standards and guidelines specifying certain provisions. ESMA published a first consultation package in July 2023, a second in December 2023 and two additional standalone consultation papers in January 2024. This latest consultation package (no. 3) includes all remaining mandates with an 18-month deadline. The aim of these public consultations is to collect views, comments, and opinions from stakeholders, investors and market participants on the appropriate implementation of MiCA.

Contents

This paper contains 4 sections (chapters 3 – 6) relating to the four mandates under consultation: (i) prevention and detection of crypto-asset market abuse; (ii) suitability requirements applicable to the provision of advice and portfolio management services in crypto-assets and the format of the periodic statement to be provided for portfolio management services; (iii) transfer services for crypto-assets; and (iv) maintenance of systems and security access protocols. An aggregated list of consultation questions can be found in Annex I. Annex II includes the draft RTS and guidelines.

Next Steps

ESMA aims to close the public consultation respecting legal deadlines as set out in MiCA. ESMA will consider the feedback received during this consultation and expect to publish a final report and submit the draft technical standards to the European Commission for endorsement by December 2024.

2 Introduction

1. The Regulation on Markets in Crypto-assets (MiCA)[1] was published in the Official Journal on 9 June 2023 and entered into force on 29 June 2023.

2. MiCA requires ESMA to develop a series of RTS, ITS and Guidelines, in close cooperation with the EBA. This consultation package covers one draft RTS and three draft guidelines on: (i) arrangements, systems and procedures for detecting and reporting suspected market abuse (RTS); (ii) suitability requirements applicable to the provision of advice on crypto-assets and portfolio management of crypto-assets and the format of the periodic statement referred to in Article 81(14) of MiCA (guidelines); (iii) the procedures and policies, including the rights of clients, in the context of transfer services of crypto-assets (guidelines); and (iv) maintenance of systems and security access protocols in conformity with appropriate Union standards (guidelines).

3. The technical standards in this consultation paper should be submitted by ESMA to the European Commission by 30 December 2024.

4. While this Consultation Paper does not include a draft cost-benefit analysis, ESMA has developed its draft RTS and guidelines having due regard to the principle of proportionality and being mindful about the possible costs the obligations they contain would create for market participants. ESMA considers that the provisions included in the draft RTS and guidelines in the Annex of this paper do not create new costs for concerned market stakeholders beyond the ones that naturally stem from the Level 1 obligations. Nevertheless, respondents are invited to highlight in their response any specific concerns the ESMA proposals could raise for them in terms of their associated costs in order to contribute to the cost-benefit analysis to be published in the final report on the RTS and guidelines covered in this consultation paper.

[1] Regulation (EU) 2023/1114 of the European Parliament and the Council of 31 May 2023 on markets in crypto-assets (OJ L 150, 9.6.2023, p. 40–205)

3 Arrangements, systems and procedures for detecting and reporting suspected market abuse in crypto-assets

3.1 Background

Article 92(2) of MiCA:

"ESMA shall develop draft regulatory technical standards to further specify:

(a) appropriate arrangements, systems and procedures for persons to comply with paragraph 1;

(b) the template to be used by persons to comply with paragraph 1;

(c) for cross-border market abuse situations, coordination procedures between the relevant competent authorities for the detection and sanctioning of market abuse"

5. Title VI of MiCA establishes rules to deter market abuse with respect to trading of crypto-assets. As part of these rules, MiCA prohibits insider dealing, unlawful disclosure of inside information and market manipulation, and includes specific obligations for the prevention and detection of abusive behaviours.

6. More precisely, Article 92(1) of MiCA requires that persons professionally arranging or executing transactions (PPAETs) in crypto-assets should have in place effective arrangements, systems and procedures to prevent and detect market abuse. In addition, MiCA requires PPAETs to report to the competent authority of the Member State where they are registered or have their head office (or in the case of a branch, the Member State where the branch is situated) any reasonable suspicion regarding an order or transaction as well as other aspects of the functioning of the distributed ledger technology, such as the consensus mechanism, where there might be circumstances indicating the existence of market abuse.

7. Article 92(1), second subparagraph, also foresees that competent authorities receiving a suspicious transaction or order report (STOR) should transmit such information immediately to the competent authorities of the trading platforms concerned.

8. In addition, Article 92(2) of MiCA mandates ESMA to draft an RTS to further specify: (a) appropriate arrangements, systems and procedures for persons to comply with Article 92(1); (b) the template to be used by persons to comply with Article 92(1); (c) for cross-border market abuse situations, coordination procedures between the relevant competent authorities for the detection and sanctioning of market abuse.

3.2 Assessment

9. To render the STOR regime under MiCA effective, it is crucial to further specify the elements needed for PPAETs to comply with the regime as well as the coordination procedures between NCAs in case of cross-border market abuse, as required by the mandate under Article 92(2) of MiCA. In doing so, ESMA notes that the framework designed under MiCA as well as the empowerment for ESMA to develop a draft RTS in accordance with Article 92(2) of MiCA, resembles, respectively, the obligation and the mandate under Article 16 of Regulation (EU) No 596/2014[2] (MAR) on STORs for financial instruments.

10. To recall, MAR establishes a two-fold obligation for i) market operators and investment firms operating a trading venue which are required to prevent, detect and report STORs to NCAs and ii) for PPAETs which should detect and report STORs to NCAs. In addition, the empowerment under Article 16(5) of MAR mandated ESMA to develop an RTS to determine appropriate arrangements, systems and procedures as well as the template to comply with the STOR regime, eventually resulting in Commission Delegated Regulation (CDR) 2016/957[3].

11. Against this background, ESMA's preliminary view is that Article 16 of MAR and CDR 2016/957 can be taken as a precedent for the mandate on the arrangements, systems, and procedures for PPAETs to prevent and detect market abuse, and on the STOR template.

12. With respect to the third element of the mandate under Article 92(2) of MiCA referring to the coordination procedures between NCAs for the detection and sanctioning of cross-border market abuse situations, ESMA considers that, despite this mandate being new compared to Article 16 of MAR, Commission Implementing Regulation (CIR) 2020/1406[4] developed under MAR can also be taken as a reference as it addresses the cooperation procedures, unsolicited cooperation or exchange of information, or the restrictions and permissible uses of information between competent authorities.

3.2.1 Appropriate arrangements, systems, and procedures

13. In order to effectively design the appropriate arrangements, systems, and procedures for complying with the regime, ESMA considers it necessary to first analyse the

[2] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC.
[3] Commission Delegated Regulation (EU) 2016/957 of 9 March 2016 supplementing Regulation (EU) No 596/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the appropriate arrangements, systems and procedures as well as notification templates to be used for preventing, detecting and reporting abusive practices or suspicious orders or transactions.
[4] Commission Implementing Regulation (EU) 2020/1406 of 2 October 2020 laying down implementing technical standards with regard to procedures and forms for exchange of information and cooperation between competent authorities, ESMA, the Commission and other entities under Articles 24(2) and 25 of Regulation (EU) No 596/2014 of the European Parliament and of the Council on market abuse.

personal scope of the obligation to submit STORs as well as the type of orders, transactions and behaviours that should be reported by means of a STOR.

Personal scope of the Article 92 regime

14. Article 92 of MiCA imposes the obligation to have arrangements, systems and procedures to prevent, detect and report to NCAs possible market abuse cases on PPAETs. On the contrary, Article 16 of MAR differentiates by establishing the obligation for market operators and investment firms that operate a trading venue to prevent, detect and report, and for PPAETs to only detect and report STORs.

15. While MiCA does not provide a definition of PPAETs, MAR defines a PPAET under Article 3(28) as "a person professionally engaged in the reception and transmission of orders for, or in the execution of transactions in, financial instruments". Moreover, this concept was addressed by an ESMA Q&A[5], making clear that the definition of PPAETs should be read in a broad sense, encompassing buy-side firms, proprietary traders, DEA providers and non-financial firms that trade on their own account as part of their business activities.

16. Given the broad scope of the reference "person professionally arranging and executing transactions", ESMA is of the view that while CASPs operating a trading platform[6] are not mentioned in Article 92(1) of MiCA, they should nevertheless be considered PPAETs and should therefore be subject to the regime foreseen in Article 92 of MiCA. This is in line with Article 76(7)(g) of MiCA, according to which CASPs operating a trading platform should have in place systems, procedures and arrangements to ensure that their trading systems are able to prevent and detect market abuse, which they have to document when applying for authorisation[7].

17. As a result, the mandate in Article 92(2) of MiCA should be read as also covering CASPs operating a trading platform.

---

[5] MAR Q&A 6.1: The definition of "person professionally arranging or executing transactions" laid down in point (28) of Article 3(1) of MAR is activity based, does not cross refer to definitions under MiFID and is independent from the latter, leading thus to consider that the scope of Article 16(2) of MAR is not only limited to firms or entities providing investment services under MiFID. In the absence of any reference in the definition that would limit the scope and exclude particular categories of persons regulated by other financial European legislation, ESMA considers that the obligation to detect and identify market abuse or attempted market abuse under Article 16(2) of MAR applies broadly, and "persons professionally arranging or executing transactions" thus includes buy side firms, such as investment management firms (AIFs and UCITS managers), as well as firms professionally engaged in trading on own account (proprietary traders) and investment firms providing direct electronic access (DEA providers) with respect to their DEA clients' trading activity. Non-financial firms that, in addition to the production of goods and/or services, trade on own account in financial instruments as part of their business activities (e.g. industrial companies for hedging purposes) can be considered firms professionally arranging or executing transactions in financial instruments under Article 16(2) of MAR. The fact that they have staff or a structure dedicated to systematically deal on own account, such as a trading desk, or that they execute their own orders directly on a trading venue as defined under MiFID II, are indicators to consider a non-financial firm as a person professionally arranging or executing transactions. It is reminded that detecting and reporting suspicious orders and transactions under Article 16(2) of MAR should be applied by "persons professionally arranging or executing transactions" through the implementation of arrangements, systems and procedures that are appropriate and proportionate to the scale, size and nature of their business activity

[6] Article 3(1)(16) MiCA.

[7] Article 62(2)(n) of MiCA.

Material scope of the prevention and detection mechanism

18. Firstly, when comparing Article 92 of MiCA with Article 16 of MAR, it becomes evident that MAR only refers to the obligation to submit STORs in relation to "an order or transaction in any financial instrument, including any cancellation or modification thereof" while Article 92 of MiCA extends the obligation to report as a STOR any "order or transaction, including any cancellation or modification thereof, and other aspects of the functioning of the distributed ledger technology such as the consensus mechanism".

19. Secondly, ESMA notes that MiCA is clear when indicating that orders, transactions, and other aspects of the distributed ledger technology may suggest the existence of market abuse e.g., the well-known Maximum Extractable Value (MEV) whereby a miner/validator can take advantage of its ability to arbitrarily reorder transactions to front-run a specific transaction(s) and therefore make a profit.

20. Differently, ESMA is of the view that other types of fraud such as scams, payments fraud or account takeover are not subject to compulsory notification to NCAs under Article 92 of MiCA in the absence of an identifiable connection with market abuse[8].

21. ESMA would like to remark that this limitation in the scope does not affect national laws and regulations obliging persons to notify public authorities (such as public prosecutors) about possible administrative or criminal infringements.

Arrangements, systems and procedures

22. After having analysed the scope of the obligation under Article 92, it is useful to assess what should be the appropriate arrangements, systems, and procedures for PPAETs to comply with the obligation to prevent and detect market abuse in crypto-assets. As mentioned in the introductory section, ESMA considers that CDR 2016/957 can be taken as a precedent for this mandate considering the similarities between the empowerments received under Article 92(2) of MiCA and Article 16(5) of MAR.

23. From that starting point, ESMA considers that the proposed technical standard should add elements related to the specific nature of transactions in crypto-assets, such as the effective and ongoing monitoring of the functioning of the distributed ledger technology, including the consensus mechanism.

24. Nevertheless, ESMA is of the view that some of the requirements imposed to PPAETs and trading venues under CDR 2016/957should also be extended to PPAETs dealing in crypto-assets, considering that the majority of abusive behaviours occurring in

[8] ESMA staff consider this point important because the IOSCO consultation paper on Policy Recommendations for crypto and digital asset markets extend the market surveillance requirements applying to CASPs beyond market abuse strictly speaking. Examples of these requirements are that CASPs should be required to have "requirements, in line with FATF recommendations for AML-CTF, including (amongst other things) customer due diligence requirements".

crypto-asset markets appear to follow patterns and schemes already observed in the traditional financial instrument's space.

25. In particular, as further outlined in section 3.2.1, ESMA considers that systems, arrangements, and procedures should be developed around the principle of proportionality in relation to size and nature of business activity and the risk that these activities pose to the market. In that respect, they should be designed to allow PPAETs to adequately prevent and detect any suspicious activity and to report it to the relevant NCA in a timely fashion.

3.2.2 STOR template

26. As is the case under MAR, ESMA considers that the template should include a number of fields allowing for the identification of the person submitting the STOR as well as the transaction or order concerned, the description of the suspicion and, where possible, the identity of the suspected person.

27. The template should also provide for additional information and supporting documentation that might be useful in the context of the report. In addition, it is important to note that the template should be adapted to reflect specificities of the crypto-asset markets such as the identification of the crypto-asset (including the type of crypto-asset and/or the trading pair) or of the type of DLT technology used when the reported behaviour relates to aspects connected with the functioning of the DLT.

3.2.3 Coordination procedures between competent authorities for detection and sanctioning of cross-border market abuse

28. With respect to the coordination procedures, ESMA notes that MiCA refers to "cross-border market abuse situations" without defining them. In this context, ESMA would deem it worth specifying in the RTS, without being overly prescriptive, what cross-border market abuse situations are and what they entail. For instance, this could refer, but not be limited to, cases where the abusive behaviour is perpetrated by an individual on a territory different from the one where the crypto-asset is traded.

29. Other cases could be market abuse committed from a different jurisdiction than the one where the CASP is registered or market abuse cases perpetrated through a CASP licensed and operating in more than one Member State. This aspect appears of relevance also considering that crypto-assets markets are global and thus inherently cross-border.

30. In addition, ESMA has taken advantage of the experience gathered since the implementation of MAR. That experience shows that, in general, coordination and cooperation between NCAs for the monitoring and enforcement of market abuse works well. On that basis, ESMA understands that the draft technical standard must address a limited number of parameters, such as the identification of the situations in which a

certain degree of coordination is necessary, without the intention to exhaust all the possibilities as explained in the previous paragraphs.

31. Moreover, in ESMA's view, a coordination procedure for sanctioning of market abuse and the general principle of "ne bis in idem" should ensure that only one NCA eventually enforces a market abuse breach. This may cover the early assessment as to the determination of NCAs' competence in the very case, the identification of potential multiple NCAs' competence and the necessary interactions to avoid duplication of supervisory actions. This should also include ESMA's role in coordinating investigative or enforcement activities started by two or more competent authorities, when requested by any of them.

32. As corollary of that principle, the proposal foresees the possibility for an NCA receiving information on a market abuse case which may fall outside of its area of competence to forward that information to the potentially relevant NCA(s).

33. As regards the template to be used to transmit STORs that would fall under the competence of another NCA, Article 95 of MiCA already mandates ESMA to develop an ITS to further specify the information to be exchanged between competent authorities in order to cooperate in investigation, supervision, and enforcement activities in general. ESMA considers that this case is sufficiently covered by that technical standard.

3.3 Proposal

34. ESMA has developed the draft RTS considering the similarities between the MAR and MiCA provisions and mandates regarding the STOR regime. Furthermore, while differences between financial instruments and crypto-assets markets exist, also in relation to the type of players operating in these markets, ESMA would still see merit in aligning the regime for prevention and detection of market abuse as well as for reporting of STORs under MAR and MiCA to leverage on the experience developed under MAR. Hence, the part of the RTS dealing with appropriate arrangements, systems and procedures as well as the notification template has been largely based on CDR 2016/957, with the addition and adaptation of some provisions targeting features which are specific to the crypto environment.

35. At the same time, ESMA has leveraged on CIR 2020/1406 with respect to the mandate on coordination procedures between competent authorities for detection and sanctioning of cross-border market abuse situation.

36. In that light, the following sections provide an overview of ESMA's proposals about the content of the technical standard while the draft RTS is presented in Annex II below.

3.3.1 Appropriate arrangements, systems and procedures

Personal scope of the Article 92 regime

37. Based on the analysis presented in section 3.2.1 and consistent with the MAR precedents, ESMA proposes that the following persons should be considered as PPAETs for the purpose of Article 92 of MiCA:

    a. CASPs operating a trading platform[9];

    b. CASPs providing services related to crypto-assets such as reception or transmission of orders for crypto-assets on behalf of clients, execution of orders for crypto-assets on behalf of clients, portfolio management of crypto-assets, exchange of crypto assets for funds, exchange of crypto-assets for other crypto assets[10];

38. Persons dealing on own account in crypto-assets on a professional basis or as part of their business activity. The fact that they have staff or a structure dedicated to systematically deal on own account, such as a trading desk are indicators to consider a person as a PPAET.

39. This reading is reflected in the recitals of the draft RTS presented in Annex II below.

Q1: 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.

Material scope of prevention and detection mechanisms

40. Based on the analysis of the legal text presented in section 3.2.1, ESMA concludes that transactions, orders, and other aspects of the functioning of the distributed ledger technology should be reported by means of a STOR only when they are suspected to constitute market abuse.

Arrangements, systems and procedures

41. In line with the precedent identified and based on the analysis presented in section 3.2.1, ESMA considers that the draft technical standard should require PPAETs to establish arrangements, systems and procedures that ensure an effective and on-going monitoring of transactions, orders and other aspects of the functioning of the distributed ledger technology and allow for the reporting of STORs to the relevant NCA. Considering that the size, nature and scale of the business activity carried out by PPAETs may vary significantly, it is important to ensure that systems, arrangements and procedures developed by PPAETs are proportionate and appropriate to comply

[9] See recital (21) of MiCA.
[10] See recital (21) of MiCA.

with the STOR regime. It is also important that these systems and procedures are adequately calibrated to the risk dimension of the activities carried out by PPAETs.

42. At the same time, ESMA considers that these systems, arrangements, and procedures should be updated regularly to ensure that they remain fit for purpose. Therefore, the RTS introduces a requirement for PPAETs to assess them regularly, at least on an annual basis, and update them when necessary. In addition, the draft RTS requires PPAETs to document in writing what those systems, arrangements and procedures are and to keep track of any changes or updates.

43. In the draft RTS, ESMA also proposes that those systems should have certain technical capabilities, such as the possibility to replay and analyse order book data, but also to operate in an algorithmic trading environment. This appears of relevance considering the technological development and the concrete possibility that these markets attract participants deploying algorithmic trading strategies.

44. Furthermore, such systems, arrangements and procedures should cover the full range of trading activities undertaken by PPAETs and should allow PPAETs, to analyse every transaction executed and order placed, modified, cancelled, or rejected in the systems, both on and outside of a trading venue. Similarly, CASPs operating a trading platform should also develop systems that allow for the analysis of every order entered or transaction concluded on their platforms.

45. To ensure that PPAETs are able to analyse behaviours that might constitute market abuse in a timely manner, the draft RTS also require PPAETs' systems and arrangements to produce alerts indicating a suspicious activity. Those alerts should serve as a basis for any further analysis of a suspicious behaviour.

46. Relatedly, in line with the MAR precedent, ESMA remains of the view that an appropriate level of human analysis in the monitoring, detection and identification of the suspected behaviour should be ensured. Considering the importance of the staff involved in the prevention and detection of market abuse, they should also receive dedicated trainings, which should take place on a regular basis.

47. ESMA also considers that PPAETs may delegate their prevention and detection activity, including the performance of data analysis and generation of alerts, to a third party or to a person of the same group. However, to ensure that PPAETs remain in control of those functions, the draft RTS sets out some necessary requirements, such as the existence of a written agreement between the parties and the retention of access to the relevant information and the necessary expertise so the PPAET may assess the work conducted by the delegated party.

48. PPAETs might analyse orders, transactions and other aspects of the functioning of the DLT but conclude that a STOR should not be submitted. To ensure that PPAETs have the necessary information to elaborate on the analysis carried out, the draft RTS

requires them to maintain information on the suspicious behaviour for a period of five years and to provide it to the relevant NCA upon request.

49. Lastly, to enable NCAs to investigate STORs in a timely fashion, ESMA also proposes that STORs should be submitted without delay, as soon as a reasonable suspicion is formed, noting that additional information might be submitted at a later stage if needed. The means for transmitting such a STOR are the electronic ones specified by the relevant NCA.

50. These requirements are included in Section 1 of the draft RTS presented in Annex II.

Q2: 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.

3.3.2 STOR template

51. PPAETs should make use of the template included in the Annex of the draft RTS to report a STOR to the relevant NCA. It is important that the information is provided in a clear and accurate manner to enable NCAs to act upon the STOR, where relevant.

52. On substance, ESMA considers that the template should allow for the identification of the person submitting the STOR, including name, position within the reporting entity, name of the reporting entity, capacity in which the STOR is submitted, capacity of the entity with respect to the orders, transactions or behaviour and other information such as the type of trading activity carried out.

53. The template should then allow for the identification of the suspicious transaction or order as well as behaviour related to the functioning of the distributed ledger technology. In this context, ESMA notes that some relevant fields should include the description of the crypto-asset (i.e. nature of crypto-asset, trading pair, etc), the DLT used as well as the description of the suspected behaviour. The template should also provide for some other details including time and location of the suspected activity.

54. While it might be challenging to identify the person responsible for the suspicious orders/transactions/behaviour, PPAETs are also required to include information on such person(s), including name, address, date of birth, account numbers and others, when known.

55. Lastly, the template should also provide for additional documentation and additional information as needed. This might include any background or any other information considered by the PPAET that would be relevant to the report as well as any documents (email, recording of conversation, etc) that might help NCAs to investigate the case.

56. The template is presented in the Annex of the draft RTS. However, considering the differences also in taxonomy between financial instruments and crypto-asset markets,

ESMA is keen to receive feedback from the industry regarding the parameters and naming conventions that would be more adequate to identify suspicious orders, transactions or the functioning of the distributed ledger technology and any references that might be obsolete in relation to crypto-assets.

Q3: Do you agree with the proposed STOR template as presented in the Annex of the RTS?

Q4: 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?

Q5: 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?

Q6: Is there any other element or information relevant to crypto-asset markets that in your view should be included in the template? Please explain.

3.3.3 Coordination procedures between competent authorities for the detection and sanctioning of cross-border market abuse

57. With respect to the coordination procedures between competent authorities for detection and sanctioning of cross-border market abuse situation, ESMA considers that the draft technical standard should:

a. provide a non-exhaustive list of cases that would constitute cross-border market abuse. This appears of relevance considering that this concept is not defined under MiCA;

b. provide for an efficient coordination procedure for the detection of cross-border market abuse, in particular by requiring a timely exchange of information that ensures that all the NCAs potentially involved have all the elements to decide whether to pursue a potential investigation or not;

c. specify the procedure, timing and form for the exchange of STORs between competent authorities and cross-refers to the template for unsolicited exchange of information set out in the ITS under Article 95(11) of MiCA for such purpose;

d. include some provisions, in line with the mandate in Article 92(2) of MiCA, regarding coordination procedures for sanctioning of those forms of market abuse. In particular, competent authorities should report the status of preliminary assessments to any other competent authorities concerned in case of (suspected) cross-border market abuse cases and these NCAs should update each other and coordinate their supervisory actions.

e. require competent authorities to inform other NCAs involved of the start of an investigation, enforcement activity or criminal investigation and may also inform ESMA thereof. The draft RTS also foresees the possibility for ESMA to coordinate investigations and enforcement activity started by two or more competent authorities and when requested by any of these authorities.

Q7: 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.

4 Aspects of the suitability requirements applicable to the provision of advice and portfolio management in crypto-assets and the format of the periodic statement referred to in Article 81(14) of MiCA

4.1 Background

Article 81(15) of MiCA:

ESMA shall, by 30 December 2024, issue guidelines in accordance with Article 16 of Regulation (EU) No 1095/2010 specifying:

(a) the criteria for the assessment of client's knowledge and competence in accordance with paragraph 2;

(b) the information referred to in paragraph 8; and

(c) the format of the periodic statement referred to in paragraph 14.

Suitability

58. The assessment of suitability is an important investor protection requirement under MiCA. It applies to the provision of advice on crypto-assets (whether independent or not) and portfolio management of crypto-assets. In accordance with the obligations set out in paragraphs 1, 8 and 10 to 13 of Article 81 of MiCA, crypto-asset service providers providing advice on crypto-assets or portfolio management of crypto-assets have to provide suitable recommendations to their clients or have to make suitable investment decisions on behalf of their clients.

59. Article 81(15) of MiCA gives ESMA a mandate to issue guidelines on the following aspects of the suitability requirements under MiCA: (i) the criteria for the assessment of client's knowledge and competence; and (ii) the information that crypto-asset service providers shall obtain from their clients or prospective clients regarding their knowledge of, and experience in, investing (including in crypto-assets), their investment objectives (including risk tolerance), their financial situation (including their ability to bear losses), and their basic understanding of the risks involved in purchasing crypto-assets, so as to enable crypto-asset service providers to recommend to clients or prospective clients whether or not the crypto-assets are suitable for them and, in particular, are in accordance with their risk tolerance and ability to bear losses.

60. ESMA, in accordance with the mandate it has received under Article 81(15)(a) and (b) addresses the above 2 points in the draft guidelines presented in Annex II. ESMA is however of the view that further aspects of the suitability requirements under MiCA are

worthy of guidance to ensure a consistent and harmonised application of the requirements in the area of suitability, so as to strengthen investor protection, a key objective of ESMA. ESMA therefore chose to complement the guidelines that will be issued on the basis of the mandate in Article 81(15) of MiCA by own-initiative guidelines based on Article 16(1) of the ESMA Regulation. Hence, the draft guidelines also deal with topics such as the importance of the information provided to clients about the suitability assessment or the necessary arrangements to ensure the suitability of an assessment.

61. In addition, ESMA chose to take the ESMA Guidelines on certain aspects of the MiFID II suitability requirements[11] (the "MiFID II guidelines") as a basis for the draft guidelines presented in Annex II. This is because the MiCA suitability requirements obey to the same principles as, and are very similar to, the suitability requirements provided by Directive 2014/65/EU on Markets in Financial Instruments (MiFID II), in relation to which ESMA has built extensive guidance.

62. ESMA is of the view that some principles provided in the MiFID II guidelines should apply to market participants providing advice or portfolio management services, be it in relation to financial instruments (under MiFID II) or crypto-assets (under MiCA). Clients should also benefit from the same level of protection when they invest in financial instruments and/or in crypto-assets, especially as such services may be provided by the same entity engaging in activities related to both categories of investment products.

63. ESMA is of the view that such approach is in line with MiCA as the suitability requirements provided in MiCA are almost identical to the MiFID II requirements, although less detailed.

64. For the purpose of the draft guidelines presented in Annex II, ESMA however considered and adapted the MiFID II guidelines through the prism of crypto-assets markets. For instance, under MiFID II, the extent of the obligations of an investment firm under the suitability requirements may vary depending on the level of complexity and riskiness of the financial instruments considered as part of the advice or portfolio management services. Under MiCA, such differentiation is less relevant as there is no such thing as a 'safe' crypto-asset.

65. The main differences between the MiFID II guidelines and the draft guidelines presented in Annex II are flagged in the section "Assessment" below.

[11] ESMA35-43-1163

Periodic statement for portfolio management services

66. Under Article 81(14) of MiCA, crypto-asset service providers providing the service of portfolio management of crypto-assets shall provide to their clients periodic statements of the portfolio management activities carried out on their behalf.

67. This periodic statement should include a fair and balanced review of the activities undertaken and of the performance of the portfolio during the reporting period, an updated statement of how the activities undertaken meet the preferences, objectives and other characteristics of the client, as well as an updated information on the suitability assessment referred to in paragraph 1 or its review under paragraph 12.

68. This periodic statement is to be provided at least every 3 months, unless the client has access to an online system where up-to-date valuations of the client's portfolio and updated information on the suitability assessment referred to in paragraph 1 can be accessed. The crypto-asset service provider must however have evidence that the client has accessed a valuation at least once during the relevant quarter.

69. Article 81(15)(c) of MiCA gives mandate to ESMA to issue guidelines on the format of the periodic statement referred to in Article 81(14) of MiCA.

4.2 Assessment

4.2.1 Suitability requirements

70. As explained above, ESMA chose to largely base the MiCA suitability guidelines presented hereto in Annex III off the MiFID II guidelines. This is because the MiCA suitability requirements are also largely based off the MiFID II suitability requirements.

71. However, the draft MiCA suitability guidelines in Annex III deviate from the MiFID II guidelines on a number of points, due to the specificities of crypto-assets and also some differences between the MiFID II and MiCA frameworks. For instance, some suitability requirements included in the MiFID II Delegated Regulation have been translated into guidelines applicable to crypto-assets and integrated in the draft guidelines in Annex III, where relevant to the MiCA suitability requirements.[12]

72. The two sets of guidelines also differ in relation to sustainability preferences. The MiFID II guidelines were reviewed recently to integrate new obligations relating to sustainability preferences into the suitability requirements under MiFID II.[13] In contrast with MiFID II and the MiFID II Delegated Regulation, MiCA does not include an express

[12] For instance, paragraph 16 of Guideline 1 (*Information to clients about the purpose of the suitability assessment and its scope*) of the draft guidelines in Annex III corresponds to Article 54(1) of the MiFID II Delegated Regulation.
[13] Delegated Regulation (EU) 2021/1253 as regards the integration of sustainability factors, risks and preferences into certain organisational requirements and operating conditions for investment firms, which was part of the Commission 's Action Plan 'Financing Sustainable Growth', published in March 2018.

obligation to collect information on clients' or potential clients' sustainability preferences.

73. ESMA thus did not include in the draft guidelines presented in Annex III the new additions relating to sustainability preferences that were introduced in the latest version of the MiFID II guidelines.

74. However, paragraph 27 of Guideline 2 (*Arrangements necessary to understand clients*) of the draft guidelines in Annex III suggests, at this stage, that it could be a good practice for crypto-asset service providers to collect information about the preferences on environmental, social and governance factors of the client or potential client.

Information to clients about the purpose of the suitability assessment and its scope (Guideline 1)

75. Article 81(10) of MiCA provides that crypto-asset service providers providing advice on crypto-assets or portfolio management of crypto-assets shall establish, maintain and implement policies and procedures to enable them to collect and assess all information necessary to conduct the suitability assessment referred to in Article 81(1) for each client. They shall also take all reasonable steps to ensure that the information collected about their clients or prospective clients is reliable.

76. ESMA is of the view that, to enable crypto-asset service providers to collect all the necessary information to conduct the suitability assessment and to ensure that the information collected is reliable, it is essential that the clients are informed and understand why such information is requested of them. Guideline 1 provides guidance in this respect, as this is an integral part of the suitability assessment.

77. Guideline 1 of the draft guidelines presented in Annex II follows Guideline 1 of the MiFID II guidelines closely. Paragraph 13 however adds that crypto-asset service providers should also explain to their clients or potential clients that, without the necessary information, they are not allowed to recommend crypto-assets or provide portfolio management of crypto-asset services. This is clear from Article 81(11) of MiCA.

78. Paragraph 16 of draft Guideline 1 also clarifies that the information provided to clients about the suitability assessment and its purpose should not be used to create any ambiguity or confusion about the crypto-asset service provider's responsibility in the process. This clarification, however, does not create any divergence from the MiFID II suitability regime as such guidance is in fact a requirement under Article 54(1) of the MiFID II Delegated Regulation.

Arrangements necessary to understand clients (Guideline 2)

79. Again, Guideline 2 of the draft guidelines presented in Annex II follows closely Guideline 2 of the MiFID II guidelines. However, it was rearranged as: (i) general Guideline 2 of the MiFID II guidelines was already (mostly) included in Article 81(10) of MiCA and (ii) the guidelines relating to the clients' sustainability preferences have been deleted, for

the reasons explained in paragraph 72 above. However, as previously mentioned above, paragraph 27 of Guideline 2 (*Arrangements necessary to understand clients*) of the draft guidelines in Annex II suggests, at this stage, that it could be a good practice for crypto-asset service providers to collect information about the preferences on environmental, social and governance factors of the client or potential client.

Extent of information to be collected from clients (proportionality) (Guideline 3)

80. Guideline 3 of the draft guidelines presented in Annex II follows closely the corresponding guideline in the MiFID II guidelines but draft Guideline 3 also includes some guidance reflecting in the MiCA framework the requirements of Articles 54(2) and (5) as well as Article 55(1) of the MiFID II Delegated Regulation.

81. In addition, paragraph 39 of the draft guidelines in Annex II makes clear that crypto-assets are to be considered risky and complex products and that this should be taken into account to determine the extent of the information to be collected.

Reliability of client information (Guideline 4)

82. Guideline 4 of the draft guidelines in Annex II reflect the guidance also provided in Guideline 4 of the MiFID II guidelines, together with the requirements of Article 54(7) of the MiFID II Delegated regulation being also translated into guidance relating to crypto-assets.

83. Indeed, ESMA is of the view that it is essential that crypto-asset service providers take reasonable steps to ensure that the information provided by the client is reliable. This includes, among other things, making sure that the client is aware of the importance of providing accurate and up-to-date information, questions asked to the clients are likely to be understood, taking steps to ensure the consistency of the responses and information provided by clients.

Updating client information (Guideline 5)

84. To ensure that the information on which they base the suitability assessment is reliable, crypto-asset service providers should also ensure that they have up-to-date information.

85. This is separate from the obligation to regularly review the suitability assessment (at least every two years) under Article 81(12) of MiCA. Indeed, there may be situations where client information should be updated whilst there is no obligation to review the suitability assessment.

86. However, where the suitability assessment is reviewed in accordance with Article 81(12) of MiCA, crypto-asset service providers should make sure to carry out such review on the basis of updated information.

Client information for legal entities or groups (Guideline 6)

87. Draft Guideline 6 presented in the Annex II follows closely Guideline 6 in the MiFID II guidelines. The guidance provided under draft Guideline 6 is part of the information referred to in Article 81(8) of MiCA, where it is applicable to legal entities or groups.

88. Draft Guideline 6 has been cleared of the parts relating to categories of clients under MiFID II but completed by guidance translated from the requirements under Article 54(6) of the MiFID II Delegated Regulation.

Arrangements necessary to understand crypto-assets (Guideline 7)

89. For crypto-asset service providers to assess whether the crypto-asset services or crypto-assets are suitable for their clients or prospective clients in accordance with Article 81(1) of MiCA, crypto-asset service providers should be able to understand the crypto-assets they are recommending or including in their clients' portfolios. This includes understanding the risks and costs of the crypto-assets and crypto-asset services selected for clients or potential clients.

90. Draft Guideline 7 presented in Annex II follows closely Guideline 7 of the MiFID II guidelines but the latter has been adapted so as to be applicable to crypto-assets, was cleared of the references to sustainability factors of investment products and was completed by guidance translated from Article 54(9) of the MiFID II Delegated Regulation.

Arrangements necessary to ensure the suitability of crypto-assets or crypto-asset services (Guideline 8)

91. Draft Guideline 8 in Annex II provides guidance on how crypto-asset service providers should match clients with suitable crypto-assets and crypto-asset services, in accordance with Article 81(1) of MiCA. It follows closely Guideline 8 of the MiFID II guidelines, minus the parts relating to clients' sustainability preferences.

Costs and complexity of equivalent products (Guideline 9)

92. ESMA is of the view that the suitability assessment (matching clients with suitable crypto-assets) entails a thorough assessment of the availability of alternative investments, taking into account products' costs and complexity.

93. Draft Guideline 9 presented in Annex II follows closely Guideline 9 of the MiFID II guidelines, therefore ensuring consistency between the two regimes.

Costs and benefits of switching investments (Guideline 10)

94. In accordance with Article 66(1) and 81(1) of MiCA, where crypto-asset service providers envisage to recommend a switch to their client or undertake a switch on their behalf, they should ensure and be reasonably able to demonstrate that the expected

benefits of switching are greater than the costs. Indeed, it is not sufficient to only take into account the expected return of the current crypto-asset versus the new crypto-asset. A more thorough analysis should be carried out, taking into account, for instance, all costs and charges that will be incurred due to switching, the holding period of the investment, the risks of each investment.

95. Draft Guideline 10 in Annex II follows closely Guideline 10 of the MiFID II guidelines.

Qualifications of staff (Guideline 11)

96. In accordance with Articles 68(5) and Article 81(1) and (7) of MiCA, crypto-asset service providers providing advice on crypto-assets shall ensure that natural persons giving advice or information about crypto-assets, or a crypto-asset service, on their behalf possess the necessary knowledge and competence to fulfil their obligations.

97. ESMA believes that for the advice or portfolio management services provided to be suitable to the client, the staff involved should have an adequate level of skills, knowledge and expertise, in particular in relation to the suitability assessment process.

98. Draft Guideline 13 in Annex II provides guidance on what exactly this requirement entails and follows closely Guideline 11 of the MiFID II guidelines.

Q8: 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?

Q9: 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.

4.2.2 Periodic statement

Durable medium (Guideline 1)

99. Draft Guideline 1 presented in Annex II specifies that, to comply with Article 81(14) of MiCA, crypto-asset service providers should provide the periodic statement relating to portfolio management of crypto-assets in a durable medium.

100. Draft Guideline 1 further provides guidance on what should constitute a durable medium for the purpose of complying with Article 81(14) of MiCA. For consistency with the MiFID II framework under which a similar obligation exists for portfolio management services, draft Guideline 1 follows closely the definition of "durable medium" provided in Article 4(1)(62) of MiFID II.

Access to an online system (Guideline 2)

101. Under Article 81(14) of MiCA, crypto-asset service providers should provide the periodic statement relating to portfolio management of crypto-assets every 3 months,

unless i) the client has access to an online system where up-to-date valuations of the client's portfolio and updated information on the suitability assessment referred to in paragraph 1 of Article 81(1) of MiCA can be accessed, and (ii) the crypto-asset service provider has evidence that the client has accessed a valuation at least once during the relevant quarter.

102. In this respect, MiCA follows closely the requirements of Article 60(3) of the MiFID II Delegated Regulation. Draft Guideline 2 in Annex II provides further guidance on the conditions that such online system must meet for crypto-asset service providers to comply with Article 81(14), second subparagraph of MiCA, thereby ensuring further consistency with the MiFID II regime in this respect.

Content of the periodic statement (Guideline 3)

103. In addition to the guidelines on the format of the periodic statement, ESMA chose to also provide some high-level guidance on the nature of the information that should be provided to clients to meet the requirements of Article 81(14) of MiCA. This is so that clients of portfolio management services may have a fair and balanced view of the activities undertaken and of the performance of the portfolio during the reporting period.

Q10: Do you agree with the approach followed by ESMA regarding periodic statements provided in relation to portfolio management of crypto-assets?

4.3 Proposal

104. The draft guidelines on certain aspects of the suitability requirements and format of the periodic statement for portfolio management of crypto-assets are presented in Annex III.

5 Procedures and policies, including the rights of clients, in the context of transfer services for crypto-assets

5.1 Background

Article 82(2) of MiCA:

ESMA, in close cooperation with EBA, shall issue guidelines in accordance with Article 16 of Regulation (EU) No 1095/2010 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, in the context of transfer services for crypto-assets.

105. In accordance with Article 82(2) MiCA, crypto-asset service providers providing transfer services for crypto-assets must conclude an agreement with their clients to specify their duties and their responsibilities which must include at least the identity of the parties to the agreement, descriptions of the modalities of the transfer service provided and of the security systems used by the crypto-asset service provider, fees applied by the crypto-asset service provider, the applicable law.

106. With regards to crypto-asset service providers' policies and procedures in relation to crypto-asset transfer services, MiCA does not set out any specific requirements. Article 82(2) of MiCA, however, gives a mandate to ESMA to provide guidance on such policies and procedures, including the rights of clients.

5.2 Assessment

107. The features of the provision of transfer services of crypto-assets share some similarities with payment services, regulated under the Directive on payment services in the internal market ("PSD 2").[14, 15] Therefore, ESMA has drawn on PSD 2 provisions—where relevant—in developing the draft guidelines.

108. In addition, the Regulation on information accompanying transfers of funds and certain crypto-assets[16] (the "TFOR") also regulates transfer services of crypto-assets. It lays down rules on the information on originators and beneficiaries accompanying transfers of crypto-assets, for the purposes of preventing, detecting and investigating money laundering and terrorist financing. ESMA gave due regard to the TFOR to ensure that there was no inconsistency with the draft guidelines.

[14] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015.
[15] Recital 90 of MiCA sets out that "*some crypto-asset services, in particular […] transfer services for crypto-assets on behalf of clients, might overlap with payment services*".
[16] Regulation (EU) 2023/1113 of the European Parliament and the of the Council of 31 May 2023.

Prior general information (Guideline 1)

109. The purpose of draft Guideline 1 is to ensure that crypto-asset service providers providing transfers for crypto-assets have in place adequate policies and procedures (including appropriate tools) to provide the client with some essential information on the conditions of the provision of the service, in good time before the client enters into any agreement for the provision of crypto-asset transfer services.

110. Such information should include, for instance, information on the identity of the crypto-asset service provider, the DLT network used for the transfer of crypto-assets, the costs applicable to the service or how to initiate a transfer.

111. These procedures and policies aim at disclosing relevant pre-contractual information to the client to enable him to choose the most suitable provider of crypto-asset transfer services.

Information on individual transfers for crypto-assets (Guideline 2)

112. Draft Guideline 2 is meant to ensure that clients that have sent an instruction to transfer crypto-assets also receive important information about the transaction itself, before such a transaction becomes irreversible.

113. Such information includes (i) a brief warning if and when the crypto-asset transfer will be irreversible or sufficiently irreversible in case of probabilistic settlement and (ii) information on all charges for the crypto-asset transfer payable by the client.

114. In addition, draft Guideline 2 also clarifies that crypto-asset service providers should have appropriate policies and procedures to ensure that, after the execution of individual crypto-asset transfers, the client is provided with certain minimum information, including: a reference enabling the client to identify each crypto-asset transfer, the amount and type of crypto-assets transferred or received and all costs relating to the transfer for crypto-assets.

115. Lastly, draft Guideline 2 also addresses the information that crypto-asset service providers should provide to their clients in case a crypto-asset transfer is rejected, returned or suspended. Such information should include, for instance, the reason for the rejection, return or suspension and how to remedy such rejection, return or suspension as well as any costs incurred.

Execution times and cut-off times (Guideline 3)

116. Draft Guideline 3 clarifies that crypto-asset service providers should establish, implement and maintain adequate policies and procedures relating to a minimum set of elements of process for transferring crypto-assets. This includes maximum execution times depending on the crypto-asset transferred or the number of block confirmations

needed for the transfer of crypto-assets to be irreversible on the DLT, or sufficiently irreversible in case of probabilistic settlement, for each DLT network.

Rejection of an instruction to transfer crypto-assets or of crypto-asset transferred (Guideline 4)

117. In this draft guideline, ESMA clarifies that crypto-asset service providers should establish, implement and maintain adequate risk-based policies and procedures for determining whether and how to execute, reject, return or suspend a transfer of crypto-assets. Such policies and procedures should particularly take into account the provisions of Regulation (EU) 2023/1113 applicable to crypto-asset service providers as also specified in the EBA Guidelines preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes.

Liability of the crypto-asset service provider (Guideline 5)

118. Guideline 5 clarifies that crypto-asset service providers should establish, implement and maintain adequate policies and procedures determining the conditions for the crypto-asset service provider to be liable to clients in case of unauthorised or incorrectly initiated or executed transfers of crypto-assets.

Q11: 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.

Q12: 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.

Q13: 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?

5.3 Proposal

119. The draft guidelines on the policies and procedures in the context of transfer services for crypto-assets are presented in Annex II.

6 Maintenance of systems and security access protocols in conformity with appropriate Union standards

6.1 Background

Article 14(1)(d) of MiCA:

1. Offerors and persons seeking admission to trading of crypto-assets other than asset-referenced tokens or e-money tokens shall:

(a) act honestly, fairly and professionally;

(b) communicate with holders and prospective holders of the crypto-assets in a fair, clear and not misleading manner;

(c) identify, prevent, manage and disclose any conflicts of interest that might arise;

(d) ***maintain all of their systems and security access protocols in conformity with the appropriate Union standards.***

For the purposes of point (d) of the first subparagraph*, ESMA, in cooperation with EBA, shall by 30 December 2024 issue guidelines in accordance with Article 16 of Regulation (EU) No 1095/2010 to specify those Union standards.*

120. Article 14(1)(d) of MiCA mandates ESMA, in close cooperation with EBA, to develop guidelines related to how offerors and persons seeking admission to trading of crypto assets other than asset-referenced tokens (ARTs) and e-money tokens (EMTs) (henceforth referred to collectively as 'offerors and persons seeking admission to trading') "shall […] maintain all of their systems and security access protocols in conformity with the appropriate Union standards".

121. This mandate appears under Title II of MiCA, which relates to crypto-assets other than ARTs or EMTs. It is one obligation of several found in the same paragraph of Article 14 which requires offerors to (i) act fairly and professionally, (ii) communicate with prospective holders of the crypto asset in a clear manner, and (iii) disclose conflicts of interest.

122. Further background on the mandate can be found in Recital 38 of MiCA, which says offerors and persons seeking admission to trading should have "effective administrative arrangements to ensure that their systems and security protocols meet Union standards". ESMA staff interpret 'administrative arrangements' as processes (which may involve the senior management of the offeror or person seeking admission to trading) to assign roles and access rights, as well as procedures for granting and revoking access. It is also worth noting that the formulation of 'security protocols' in the recital differs from 'security access protocols' in the mandate. ESMA considers this difference immaterial.

123. This consultation paper aims to clarify how ESMA has prepared these guidelines to further specify the provision, and to provide more detailed guidance for offerors and persons seeking admission to trading based on precedents in other technical standards at the EU level as well as international standards (ISO) for access control protocols of ICT systems.

6.2 Assessment

Assessment of the mandate under MiCA

124. The definition of 'offeror', found in Article 3(1)(13) of MiCA says, "a natural or legal person, or other undertaking, or the issuer, who offers crypto-assets to the public". The activity of "offer to the public" in paragraph 12 of the same article is defined as a "communication to persons in any form, and by any means, presenting sufficient information on the terms of the offer and the crypto-assets to be offered so as to enable prospective holders to decide whether to purchase those crypto-assets". There is no equivalent definition for 'persons seeking admission to trading' in the same article but the concept should be generally understood as it appears throughout the recitals.

125. Unlike crypto-asset service providers (CASPs), offerors of crypto-assets and persons seeking admission to trading are not in scope of Regulation (EU) 2022/2554 (DORA), which means they are not subject to the requirements for maintenance of ICT systems set out in the upcoming technical standards for a risk management framework (RMF)[17]. Nor will offerors and persons seeking admission to trading be subject to MiCA measures in the pending technical standards on regularity and continuity of services for CASPs (the mandate in Art. 68(10)(a) of MiCA)[18].

126. Elsewhere in MiCA, issuers of asset-referenced tokens (ARTs) are subject to a nearly identical set of obligations as the one for the entities in scope of this mandate. This can be found in Article 34(6) of MiCA, which requires issuers to maintain their systems and security access protocols "in conformity with appropriate Union standards". However, EBA does not have the same mandate to clarify the provision on security access protocols (though there is a broader mandate for guidelines on other measures such as risk monitoring tools, business continuity, and audits). In the preparation of these guidelines, ESMA is seeking to align with the EBA guidelines for issuers (where necessary), noting that the latter are still in draft form at the date of the publication of this consultation. However, any alignment should recognise that this mandate is far narrower than the mandate applied to issuers of ARTs in Article 34(13).

127. Considering the entities here will not fall under scope of either aforementioned sets of rules in DORA or MiCA, ESMA understands this mandate should be aimed towards

[17] JC 2023 86, Draft RTS to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554, 17 January 2024 (link)
[18] ESMA75-453128700-438, Consultation Paper, Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA) - second consultation paper, 5 October 2023 (link)

ensuring offerors and persons seeking admission to trading are subject to a minimum level of ICT security requirements, proportionate to the impact of their activities on the market for crypto-assets.

128. Furthermore, the mandate mentions two elements that offerors and persons seeking admission to trading should maintain according to Union standards: 1) systems and 2) security access protocols. The term 'systems' is ambiguous in this context. It may include things like 'business processes', or it can be narrowly construed as only including ICT systems. For the purposes of these guidelines, ESMA is only considering the narrow interpretation: ICT systems. Security access protocols is a more widely understood concept which almost always includes both logical and physical access controls (based on the precedents found in similar mandates). ESMA considers the terms 'access protocols' and 'access controls' as interchangeable.

Q14. 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).

Precedent in other EU legal acts: 'appropriate Union standards'

129. ESMA, with the other ESAs, has published draft standards on ICT security access controls as part of the risk management framework (RMF) of DORA. Although those provisions found in the RMF are aimed at financial entities (a term that encompasses CASPs and issuers), most of the concepts are still fit for purpose in the context of this mandate, especially Articles 21 and 33 on access control and Article 7 on cryptographic key management. Therefore, ESMA used this draft RTS as a basis for alignment with these guidelines, calibrating for proportionality (due to the different entities under scope) and the narrower mandate under MiCA. In particular, the Simplified ICT Risk Management Framework (Article 16 of DORA), which applies a streamlined approach for smaller entities under scope (e.g., microenterprises and small, non-interconnected investment firms) has served as a model, although ESMA considers the MiCA mandate on ICT systems for Title II entities narrower than the requirements in Article 16 of DORA. Indeed, considering the co-legislators decided against subjecting the entities under scope of these guidelines to the full or even simplified DORA requirements, it would not be appropriate to use this mandate for that purpose.

130. Several other EU Directives include pending technical standards or guidelines intended to specify measures for access controls in the context of ICT security. Under the Network and Information Security Directive (EU) 2022/2555 (NIS2), the Commission is empowered to prepare implementing acts on the 'technical and methodological requirements' for a range of measures, including access control policies (as well as policies regarding the use of cryptography)[19]. Similarly, as part of Directive (EU) 2022/2557 (Critical Entities Regulation), the Commission is also responsible for the

[19] Commission Implementing Act pursuant to Art. 21(5) of Directive (EU) 2022/2555 (NIS2) (link)

preparation of guidelines on a range of resilience measures for so-called 'Critical Entities' which would include 'access controls[20]'.

131. Although the draft level 2 and 3 measures under NIS2, which will enter into application on 18 October 2024, are still unavailable as of the publication of this paper, ESMA will consider alignment only insofar as those implementing measures are relevant to the mandate and the area of financial services more broadly.

132. Another precedent used in the development of these guidelines is the EBA Guidelines on ICT Information Security published in 2019[21]. Despite the banking sector focus (entities in scope include payment service providers and credit institutions), ESMA borrowed from the section on 'logical security', which fits into the 'access protocols' aspect of the mandate.

133. Although there are other precedents that meet the definition of 'in conformity with appropriate Union standards', it is important to note that those standards often draw from policies developed by international standard setting organisations, which are constantly shifting to mitigate new types of ICT security risks. Indeed, nearly all of the Union standards (to a certain extent) are based in the ISO 27002 standards. Therefore, ESMA has referred to the latest (2022) edition for confirmation to ensure the controls in the guidelines are based on the latest internationally-recognised best practices for operational resilience. As a result, these guidelines do not venture far from the ISO 'source material' and should be instantly recognisable to ICT security professionals employed by the offeror or person seeking admission to trading.

Q15. 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.

6.3 Proposal

Approach to Guideline 1: Proportionality

134. ESMA considers the simple principle in Guideline 1 sufficient because proportionality is already embedded in the mandate, which recognises that the entities in scope do not pose risks to the stability of the crypto-asset market nor to investors on a scale commensurate to those same risks posed by CASPs and issuers (from an operational resilience perspective). Unlike the other entities under scope of MiCA, offerors and persons seeking admission to trading are not subject to DORA, nor does the mandate impose intensive business continuity requirements on them as in the other ICT-focused mandates for CASPs and issuers of ARTs. This distinction in the Level 1 text of MiCA

[20] Commission Implementing Act pursuant to Art. 13(5) of Directive (EU) 2022/2557 (Critical Entities Regulation) (link)
[21] EBA/GL/2019/04 Final Report: EBA Guidelines on ICT and security risk management, 29 November 2019 (link)

informs how ESMA prepared not just the principle in Guidelines 1, but the entire set of guidelines.

135. Nevertheless, the proportionality principle in Guideline 1 should not change the minimum requirements outlined in MiCA. All provisions within the guidelines are subject to the principle of proportionality, meaning that they should be applied in a manner that is appropriate, considering the specificities of the offeror or person seeking admission to trading's internal organisation and nature, and the complexity of their activities.

136. For a point of reference on proportionality, ESMA notes that Recital 27 of MiCA provides several thresholds that exempt certain SMEs or start-ups from the obligation to prepare a white paper. This applies to offerors and persons seeking admission to trading when their offers are made to fewer than 150 persons per Member State or the total issue of the public offer does not exceed EUR 1,000,000 over a period of 12 months. However, the exemption from preparing a white paper does not extend to the obligations under Article 14 in this mandate as is made explicit in Article 4(2). As such, these thresholds should be considered only as a benchmark for what constitutes an 'SME or start-up' according to the Level 1 text.

Approach to Guideline 2: Administrative arrangements

137. Since offerors and persons seeking admission to trading will not be subject to DORA, ESMA considers it necessary to include basic administrative arrangements around operational and ICT security risk management of the 'systems' and 'security access protocols' for the entities under scope. The basis for this approach taken in the guidelines can be found in Recital 38 of MiCA which specifically references "administrative arrangements".[22] At the same time, issuers of ARTs are subject to governance measures as part of the guidelines in Article 34(13). ESMA considers the omission of any mention of governance aspects in this mandate purposeful. Therefore, the guidelines do not compel the management body of the offeror or persons seeking admission to trading to create any new 'control function' within the organisation to comply.

138. In another departure from the DORA precedent, these guidelines do not require offerors and persons seeking admission to trading to first establish an RMF to organise the implementation of the provisions in Guidelines 3 and 4. Implementing a risk management framework implies certain responsibilities for the management body, and with governance elements largely absent from the mandate, ESMA has omitted this provision from the guidelines. However, paragraph 17 in Guideline 2 lists many recognisable aspects of a standard RMF that the offeror or person seeking admission to trading would have to implement.

[22] The relevant excerpt of Recital 38 is as follows: "Offerors and persons seeking admission to trading of crypto-assets … should have effective administrative arrangements to ensure that their systems and security protocols meet Union standards."

139. This guideline does borrow from existing precedent by requiring offerors and persons seeking admission to trading to ensure that the quantity and skills of their staff is adequate to support their ICT operational needs and their ICT and security risk management processes on an ongoing basis.

140. Any reference to the management body in these guidelines should be understood to also include offerors or persons seeking admission to trading that are legal persons managed by a single natural person.

141. ESMA notes that where issuers of ARTs/EMTs and crypto-asset service providers enter into the scope of these guidelines as part of their activities related to the offer or admission to trading of a crypto-asset (other than ART/EMT), they should continue to adhere to the ICT operational security frameworks which they are already subject to under other applicable sectoral legislation (e.g., Regulation (EU) 2022/2554 DORA).

Q16. 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.

Approach to Guideline 3: Physical access controls

142. For this guideline, ESMA takes inspiration from the precedent mentioned in the previous section, including the EBA 2019 Guidelines on ICT and Security Risk Management, (specifically, guideline 3.4.2. on logical security) and the Final Report for the draft RTS on the RMF in DORA (specifically, Articles 21 and 33). Considering the developments in ISO standards for ICT and security risk management since the preparation of the 2019 EBA guidelines, ESMA has updated some terminology in these guidelines to align with the latest best practices (e.g., the use of need-to-know, least privilege principles).

143. Guideline 3 calls on offerors or persons seeking admission to trading to assess the criticality of the operations or ICT systems located on their physical premises. While the procedures for conducting and documenting this criticality assessment are codified for financial entities in Article 8(1) of DORA, no such requirement exists in MiCA. Here, as is the case in the following Guideline 4, offerors or persons seeking admission to trading should make their own determinations about the criticality of an ICT system (or the premises in which it is located).

144. Offerors and persons seeking admission to trading should designate authorised personnel with access to the physical premises considered critical to the operation of the business. They should also designate which locations or physical areas of the business premises are considered critical (and the corresponding access rights for authorised personnel that would be required to enter those premises). In this case,

critical ICT assets may include data centres, or areas with sensitive ICT and information assets.

145. Entry and exit into these critical locations of operation should be recorded and monitored, in a manner similar to ICT logging. The monitoring should be commensurate to the classification of the assets and hence the criticality of the area accessed (based on the assessment of the offeror or person seeking admission to trading). It may also be necessary for the offeror or person seeking admission to trading to regularly review physical access rights to ensure that unnecessary or elapsed access rights are promptly revoked. ESMA has specified the frequency of these regular reviews consistent with DORA's risk management framework, which requires that elements of a financial entity's RMF be reviewed annually.

Approach to Guideline 4: ICT security access controls

146. Security access protocols (a standard feature of any ICT risk management framework), help to prevent unauthorised access to ICT systems, ensure the integrity of those systems and preserve the confidentiality of data, both internally and externally. Considering this is mentioned directly in the mandate, this is one of the most important and substantial set of measures found in these guidelines. In a departure from DORA, these guidelines do not mandate access control as part of a formal RMF.

147. The proposed Guideline 4 sets out the procedures offerors and persons seeking admission to trading should follow to address a range of elements, including authentication methods, access rights, logging and review of access rights. Unlike in DORA, these guidelines do not mandate the creation of a specific access control policy.

148. The guidelines for physical access control and ICT-specific access control largely mirror each other from a conceptual perspective. Again, this Guideline takes precedent from other Union standards for logical access without major deviations.

Approach to Guideline 5: Cryptographic key management

149. Here, ESMA follows the precedent in Article 7 of the draft RTS on the ICT RMF on 'cryptographic key management'. However, instead of mandating the creation of a specific policy on encryption and cryptographic controls as in the DORA draft RTS, the guidelines take a light-touch approach by ensuring the offeror or persons seeking admission to trading has designated adequate staff for managing the specific ICT and physical risks associated with the use of cryptographic keys. This is why ESMA has also added a reference to cryptographic key management in point (vii) of paragraph 17 (in Guideline 2) under the list of responsibilities to ensure proper ICT and security risk mitigation.

150. ESMA considers this an appropriate adaption of Article 7 of the draft RTS on the DORA RMF for this mandate due to the technological subject matter shared by both frameworks. Crypto-assets are by nature cryptographically secured, which renders key

management an important element of any ICT risk management framework. Although offerors and persons seeking admission to trading will not be custodians of client assets, it can be inferred that they will custody their own crypto-assets (e.g., before depositing them on a trading platform for crypto-assets) or those crypto-assets held in escrow on behalf of a token issuer. Compromise of the private keys of the offeror or person seeking admission to trading could therefore have wider repercussions in the market.

Q17. 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)?

7 Annexes

7.1 Annex I

Summary of questions

Q1: 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.

Q2: 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.

Q3: Do you agree with the proposed STOR template as presented in the Annex of the RTS?

Q4: 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?

Q5: 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?

Q6: Is there any other element or information relevant to crypto-asset markets that in your view should be included in the template? Please explain.

Q7: 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.

Q8: 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?

Q9: 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.

Q10: Do you agree with the approach followed by ESMA regarding periodic statements provided in relation to portfolio management of crypto-assets?

Q11: 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.

Q12: 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.

Q13: 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?

Q14. 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).

Q15. 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.

Q16. 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.

Q17. 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)?

7.2 Annex II

7.2.1 RTS on arrangements, systems and procedures for detecting and reporting suspected market abuse in crypto-assets

Draft of Technical Standard

COMMISSION DELEGATED REGULATION (EU) 2024/XXX

of XXXX

supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards for the appropriate arrangements, systems and procedure as well as the notification templates to be used for preventing, detecting and reporting suspected market abuse, and on the coordination procedures between the relevant competent authorities for the detection and sanctioning of market abuse in case of cross-border market abuse situations

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulation (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937[23], and in particular Article 92 (2) thereof,

Whereas:

(1) It is necessary to specify appropriate requirements for the arrangements, procedures and systems that persons professionally arranging or executing transactions in crypto-assets should have in place to prevent and detect market abuse for the reporting of orders, transactions and other aspects of the functioning of distributed ledger technology, such as the consensus mechanism, that could constitute market abuse under Regulation (EU) 2023/1114. Such requirements are critical in the prevention and detection of market abuse. They should also assist in ensuring that suspicious transaction and order reports (STOR) submitted to competent authorities are meaningful, comprehensive and useful.

[23] OJ L 150, 9.6.2023, p. 40.

(2) Persons professionally arranging or executing transactions covered by this technical standard may undertake a wide range of activities, including crypto-asset service providers operating a trading platform, providing the reception or transmission of orders for crypto-assets on behalf of clients, the execution of orders for crypto-assets on behalf of clients, providing portfolio management of crypto-assets, providing exchange of crypto assets for funds or exchange of crypto-assets for other crypto assets. In order to ensure that prevention and detection of market abuse is effective, appropriate systems should be in place to monitor orders, transactions and other aspects of functioning of the distributed ledger technology, in accordance with the scale, size and nature of the business activity of the person professionally arranging or executing transactions. The analysis of the appropriateness of the systems should include the risk that the activities of the person professionally arranging or executing transactions or its clients poses to the market.

(3) Such systems should provide for human analysis carried out by appropriately trained staff. The systems for monitoring market abuse should be capable of producing alerts in line with predefined parameters in order to allow for further analysis to be conducted on potential insider dealing, market manipulation or attempted insider dealing or market manipulation. The whole process is likely to require some level of automation.

(4) In order to facilitate and promote a consistent approach and practices across the Union in relation to prevention, detection and sanctioning of market abuse, it is appropriate to lay down detailed provisions harmonising the content of, the template for and the timing of the reporting of suspicious orders and transactions as well as other other aspects of the functioning of distributed ledger technology.

(5) Persons that are professionally engaged in arranging or executing transactions in crypto-assets should be able to delegate the prevention, monitoring, detection and identification of suspicious orders, transactions and other aspects of the functioning of distributed ledger technology, within a group or to delegate the data analysis and the generation of alerts, subject to appropriate conditions. Such delegation should make it possible to share resources, to centrally develop and maintain monitoring systems and to build expertise in the context of monitoring orders and transactions. Such delegation should not prevent the competent authorities from assessing, at any time, whether the systems, arrangements and procedures of the person to whom the functions are delegated are effective to comply with the obligation to prevent, monitor and detect market abuse. The obligation to report as well as the responsibility to comply with this Regulation and with Article 92 of Regulation (EU) No 2023/1114 should remain with the delegating person.

(6) Crypto asset service providers operating a trading platform should be considered as a subset of the persons professionally arranging or executing transactions in crypto-assets. These entities should have appropriate trading rules contributing to the prevention of market abuse. These entities should also have facilities to replay the order book in order to analyse the trading activity.

(7) A single and harmonised template for electronically submitting a suspicious transaction and order report (STOR) should assist compliance with the requirements set out in this Regulation and in Article 92 of Regulation (EU) No 2023/1114 in markets where orders and transactions are inherently cross-border. It should also facilitate the efficient sharing of information on suspicious orders and transactions between competent authorities in cross-border investigations.

(8) The relevant information fields contained in the STOR template, if completed clearly, comprehensively, objectively and accurately, should assist the competent authorities to promptly assess the suspicion and initiate relevant actions. The STOR template should therefore allow the persons submitting the STOR report to provide the information considered relevant about the suspicious orders, transactions or other aspects of the functioning of the distributed ledger technology reported and to explain the reasons for the suspicion. The STOR template should also allow to provide personal data that would make it possible to identify the persons involved in the suspicious activity and assist the competent authorities in the conduct of investigations. Such information should be provided at the outset, so that the integrity of the investigation is not compromised by the potential necessity for a competent authority to revert in the course of an investigation to the person who submitted the STOR.

(9) To facilitate the submission of a STOR, the template should allow for the attachment of documents and materials considered necessary to support the notification made, including in the form of an annex listing the orders or transactions relevant for the same report and detailling their prices and volumes. In addition, the template should also allow for the reporting of suspicious behaviours connected to the functioning of the distributed ledger technology.

(10) Persons professionally arranging or executing transactions in crypto-assets should not notify all orders received or transactions conducted that have triggered an internal alert. Such a requirement would be inconsistent with the requirement to assess on a case-by-case basis whether there are reasonable grounds for suspicion.

(11) The analysis of orders, transactions or other aspects of the functioning of the distributed ledger technology should factor in not only the internal information of the person professionally arranging or executing transactions in crypto-assets, but all the information publicly available, such as the information regarding transactions embedded in a public ledger system.

(12) The STORs should be submitted to the relevant competent authority without delay once a reasonable suspicion about the existence of market abuse has been formed. The analysis as to whether or not a given order or transaction is to be considered suspicious should be based on facts, not speculation or presumption and should be carried out as quickly as practicable. Delaying the submission of a report in order to incorporate further suspicious orders, transactions or other aspects of the functioning of the distributed ledger technology or accumulating several STORs are irreconcilable with the obligation to act without delay, where a reasonable suspicion has already been

formed. In any case the submission of a STOR should be assessed on a case-by-case basis to determine if several orders, transactions or other aspects of the functioning of the distributed ledger technology could be reported in a single STOR.

(13) There might be circumstances when a reasonable suspicion of market abuse is formed some time after the suspected activity occurred, due to subsequent events or available information. This should not be a reason for not reporting the suspected activity to the competent authority. In order to demonstrate compliance with the reporting requirements in those specific circumstances, the person submitting the report should be able to justify the time discrepancy between the occurrence of the suspected activity and the formation of the reasonable suspicion of market abuse.

(14) The ability to recall and review the analysis performed on STORs which have been submitted, as well as those suspicious orders, transactions and behaviours connected to the functioning of the distributed ledger technology which were analysed, but in relation to which it was concluded that the grounds for suspicion were not reasonable, will assist persons professionally executing or arranging transactions in crypto-assets in exercising their judgement when considering subsequent suspicious orders or transactions.

(15) The analysis performed on suspicious orders, transactions, behaviours and other aspects of the functioning of the distributed ledger technology which did not lead to a STOR assists those persons in refining their surveillance systems and in detecting patterns of repeated behaviour, the aggregate of which could, considered as a whole, result in a reasonable suspicion of market abuse. Furthermore, the above records will also assist in evidencing compliance with the requirements laid down in this Regulation and facilitate the performance by competent authorities of their supervisory, investigatory and enforcement functions under Regulation (EU) No 2023/1114.

(16) Considering that markets in crypto-assets are inherently cross-border, it is necessary to specify coordination procedures between the relevant competent authorities for the detection and sanctioning of market abuse in case of cross-border market abuse situations. These coordination procedures should ensure that there are no conflicting investigations or enforcement activities. In this context, cross border market abuse situations should include at least cases in which suspicious transactions are carried out in a Member State concerning a crypto-asset that is admitted to trading in another Member State and cases in which the relevant crypto-asset service provider is operating in more than one Member State.

(17) It is also necessary to lay down provisions for the transmission of STORs on crypto-assets among competent authorities. Such requirements are critical, in the absence of a transaction reporting regime, to ensure efficient market supervision and enforcement while preventing the transmission of a massive flow of information that would not be useful for the receiving authority.

(18) Any processing of personal data under this Regulation should be carried out in compliance with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(19) This Regulation is based on the draft regulatory technical standards submitted by the European Securities and Markets Authority to the Commission.

(20) The European Securities and Markets Authority has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested theadvice of the Securities Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and the Council.

HAS ADOPTED THIS REGULATION:

Article 1

Definitions

For the purposes of this Regulation, the following definitions shall apply:

(a) 'suspicious transaction and order report' (STOR) means the report on suspicious orders or transactions, including any cancellation or modification thereof, and other aspects of functioning of the distributed ledger technology where there might exist circumstances indicating that market abuse has been committed, is being committed or is likely to be committed;

(b) 'electronic means' are means of electronic equipment for the processing (including digital compression), storage and transmission of data, employing wires, radio, optical technologies, or any other electromagnetic means;

(c) 'group' means a group as defined in Article 2(11) of Directive 2013/34/EU of the European Parliament and of the Council[24];

(d) 'order' means each and every order, including each and every quote, irrespective of whether its purpose is initial submission, modification, update or cancellation of an order and irrespective of its type;

[24] Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 19).

(e) ‘algorithmic trading’ means trading in crypto-assets where a computer algorithm automatically determines individual parameters of orders such as whether to initiate the order, the timing, price or quantity of the order or how to manage the order after its submission, with limited or no human intervention, and does not include any system that is only used for the purpose of routing orders to one or more trading platform or for the processing of orders involving no determination of any trading parameters or for the confirmation of orders or the post-trade processing of executed transactions;

(f) ‘cross-border market abuse situations’ mean at least situations in which:

(i) more than one competent authority is competent to detect or sanction a potential market abuse case; or

(ii) cooperation between two or more competent authorities is necessary to detect, investigate or sanction a potential market abuse case.

SECTION 1

APPROPRIATE ARRANGEMENTS, SYSTEMS AND PROCEDURES TO PREVENT, DETECT AND REPORT MARKET ABUSE, AND THE TEMPLATE TO BE USED BY PERSONS PROFESSIONALLY ARRANGING OR EXECUTING TRANSACTIONS

Article 2

General requirements

1. Persons professionally arranging or executing transactions in crypto-assets shall establish and maintain arrangements, systems and procedures that ensure:

(a) effective and ongoing monitoring of all orders received and transmitted, and all transactions in crypto-assets executed, for the purposes of preventing, detecting and identifying orders and transactions that could constitute market abuse;

(b) effective and ongoing monitoring, for the purposes of detecting and identifying other aspects of the functioning of the distributed ledger technology, such as the consensus mechanism, where there might exist circumstances indicating that market abuse has been committed, is being committed or is likely to be committed;

(c) the transmission of STORs to competent authorities in accordance with the requirements set out in this Regulation and using the template set out in the Annex.

2. The obligations referred to in paragraph 1 shall apply to orders, transactions and other aspects of the functioning of the distributed ledger technology which might constitute market abuse and shall apply irrespective of:

(a) the capacity in which the order is placed or the transaction is executed;

(b) the types of clients concerned;

(c) whether the orders were placed or transactions executed on or outside a trading platform.

3. Persons professionally arranging or executing transactions in crypto-assets shall ensure that the arrangements, systems and procedures referred to in paragraphs 1 and 2:

(a) are appropriate and proportionate in relation to the scale, size and nature of their business activity;

(b) are regularly assessed, at least through an annually conducted audit and internal review, and updated when necessary;

(c) are clearly documented in writing, including any changes or updates to them, for the purposes of complying with this Regulation, and that the documented information is maintained for a period of five years.

4. Persons professionally arranging or executing transactions in crypto-assets shall, upon request, provide the competent authority with the information on the assessment referred to in point (a) and information referred to in points (b) and (c) of paragraph 3, including information on the level of automation put in place.

Article 3

Prevention, monitoring and detection

1. Persons professionally arranging or executing transactions in crypto-assets shall, to a degree which is appropriate and proportionate in relation to the scale, size and nature of their business activity, employ software systems and have in place procedures which assist the prevention and detection of market abuse.

The systems and procedures referred to in the first subparagraph shall include software capable of deferred automated reading, replaying and analysis of order book data, and such software shall have sufficient capacity to operate in an algorithmic trading environment.

2. The arrangements, systems and procedures referred to in Article 2(1) shall:

(a) cover the full range of trading activities undertaken by the persons professionally arranging or executing transactions in crypto-assets;

(b) produce alerts indicating activities requiring further analysis for the purposes of detecting potential market abuse;

(c) allow crypto-asset service providers operating a trading platform for the analysis, individually and comparatively, of each and every transaction executed, and order placed, modified, cancelled, or rejected in the systems of the trading platform;

(d) allow persons professionally arranging or executing transactions in crypto-assets for the analysis, individually and comparatively of each and every transaction executed and order placed, modified, cancelled or rejected inside and outside a trading platform. This requirement is applicable irrespective of whether or not the orders and transactions are placed and executed by means of the distributed ledger.

3. Persons professionally arranging or executing transactions in crypto-assets shall put in place and maintain arrangements and procedures that ensure an appropriate level of human analysis in the prevention, monitoring, detection and identification of transactions, orders and aspects of the functioning of the distributed ledger technology that indicate the likelihood or existence of market abuse behaviours.

4. A person professionally arranging or executing transactions in crypto-assets may delegate to a third party ('the provider') or to a legal person forming part of the same group, by written agreement, the performance of tasks relating to prevention, monitoring, detection and identification of orders, transactions or other aspects of the functioning distributed ledger technology that could constitute market abuse, including the performance of data analysis on order and transaction data, and the generation of alerts. The person delegating those tasks shall remain fully responsible for discharging all of its obligations under this Regulation and Article 92 of Regulation (EU) No 2023/1114 and shall comply at all times with the following conditions:

(a) it shall retain the expertise and resources necessary for evaluating the quality of the services provided and the organisational adequacy of the providers, for supervising the delegated services and for the management of the risks associated with the delegation of those functions on an ongoing basis;

(b) it shall have direct access to all the relevant information regarding the data analysis and the generation of alerts.

The written agreement shall contain the description of the rights and obligations of the person delegating the tasks referred to in the first subparagraph and those of the provider. It shall also set out the grounds that allow the person delegating the functions to terminate such agreement.

5. As part of the arrangements and procedures referred to in Article 2, persons professionally arranging or executing transactions in crypto-assets shall maintain the information documenting the analysis carried out with regard to orders, transactions and aspects of the functioning of distributed ledger technology that could constitute market abuse for a period of five years. That information shall include the analysis made and

the reasons for submitting or not submitting a STOR. That information shall be provided to the competent authority upon request.

Article 4

Training

Persons professionally arranging or executing transactions in crypto-assets shall organise and provide effective and comprehensive training to the staff involved in the prevention, monitoring, detection and identification of orders, transactions and other aspects of the functioning of the distributed ledger technology that could indicate the existence of market abuse, including the staff involved in the processing of orders and transactions and other aspects of the functioning of the distributed ledger technology. Such training shall take place on a regular basis and shall be appropriate and proportionate in relation to the scale, size and nature of the business.

Article 5

Reporting obligations

1. Persons professionally arranging or executing transactions in crypto-assets shall establish and maintain effective arrangements, systems and procedures that enable them to assess, for the purpose of submitting a STOR, whether an order, a transaction or other aspects of the distributed ledger technology indicate that market abuse has been committed, is being committed or is likely to be committed. These arrangements, systems and procedures shall include an appropriate level of human analysis.

2. Persons professionally arranging or executing transactions in crypto-assets shall ensure that STORs are based on facts and analysis, considering all the information available to them.

3. Persons professionally arranging or executing transactions in crypto-assets shall ensure that the arrangements and procedures referred to in Article 2 guarantee and maintain the confidentiality of the information. In particular, these persons shall have in place procedures to ensure that the person in respect of which the STOR was submitted and anyone who is not required to know about the submission of a STOR by virtue of their function or position within the reporting person is not informed of:

   (a) the generation of alerts or the assessment that may lead to the submission of a STOR. This includes that the reporting person will complete the STOR without sending requests of information to the person in respect of which the STOR may be submitted to complete certain fields.

   (b) the submission or the intention to submit a STOR to the competent authority.

Article 6

Timing of STORs

1. Persons professionally arranging or executing transactions in crypto-assets shall ensure that they have in place effective arrangements, systems and procedures for the submission of a STOR without delay, in accordance with Article 92 of Regulation (EU) No 2023/1114, once reasonable suspicion of market abuse is formed.

2. The arrangements, systems and procedures referred to in paragraph 1 shall entail the possibility to report STORs in relation to transactions, orders or other aspects of the functioning of the distributed ledger technology which occurred in the past, where suspicion has arisen in the light of subsequent events or information. In such cases, the person professionally arranging or executing transactions in crypto-assets shall explain in the STOR to the competent authority the delay between the suspected breach and the submission of the STOR according to the specific circumstances of the case.

3. Persons professionally arranging or executing transactions in crypto-assets shall submit to the competent authority any relevant additional information which they become aware of after the STOR has been originally submitted, and shall provide any information or document requested by the competent authority.

Article 7

Content of STORs

1. Persons professionally arranging or executing transactions in crypto-assets shall submit a STOR using the template set out in the Annex.

2. The persons referred to in paragraph 1 submitting the STOR shall complete the information fields relevant to the reported orders, transactions or other aspects of functioning of the distributed ledger technology in a clear and accurate manner.

Article 8

Means of transmission

1. Persons professionally arranging or executing transactions in crypto-assets shall submit a STOR, including any supporting documents or attachments, to the competent authority referred to in Article 92(1) of Regulation (EU) No 2023/1114 using the electronic means specified by that competent authority.

2. Competent authorities shall publish on their website the electronic means referred to in paragraph 1. Those electronic means shall ensure that completeness, integrity and confidentiality of the information are maintained during the transmission.

SECTION 2

COORDINATION PROCEDURES BETWEEN COMPETENT AUTHORITIES FOR DETECTION AND SANCTIONING OF MARKET ABUSE

Article 9

Coordination procedures for the detection of cross-border market abuse situations

In case of cross-border market abuse situations, the competent authority who receives the STOR shall transmit it to the other competent authorities concerned, including, where relevant, to the competent authorities of the trading platforms where the crypto-asset is admitted to trading or for which a request for admission to trading has been made.

Article 10

Procedure, timing and form for the exchange of STOR between competent authorities

1. Competent authorities shall transmit STORs by using the form of unsolicited information specified in Annex IV of Commission Implementing Regulation [XXX/XXX with regard to standard forms, templates and procedures for the cooperation and exchange of information between competent authorities]. For cross-border market abuse cases, the competent authority that receives a STOR shall transmit it to other competent authorities in accordance with Article 9 without undue delay.

2. The transmitting competent authority shall attach the STOR to the form referred to in paragraph 1, without being required to translate it into the language of the receiving competent authority. The transmitting competent authority shall include any additional documents provided in the STOR, specifying the legal basis for the provision of the information.

Article 11

Coordination procedures for the detection and sanctioning of cross-border market abuse situations

In case of cross-border market abuse situations, the following provisions apply:

(a) where a competent authority suspects that cross-border market abuse has or may have taken place, or is taking place, it shall report the status of its preliminary assessment to the other competent authorities concerned including, where applicable, the competent authorities of the trading platforms where the crypto-asset is admitted to trading. When informed about a cross-border market abuse case, the receiving competent authorities shall share information about the existence of any supervisory activity or measure or, where applicable and where such information is available to the competent authority, criminal investigation on the same case without undue delay;

(b) in presence of a cross-border market abuse case, the competent authorities concerned shall periodically update each other, inform each other of significant interim developments and coordinate their supervisory and enforcement actions;

(c) where a competent authority has formally initiated an investigation, enforcement activity or, where applicable, is aware of a criminal investigation, it shall also inform other competent authorities concerned including, where applicable, the competent authorities of the trading platforms where the crypto-asset is admitted to trading. The reporting competent authority may inform ESMA as well;

(d) where two or more competent authorities have initiated an investigation, enforcement activity or, where applicable, criminal investigation, any of them may request the coordination of ESMA at any point in time.

Article 12

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission

The President

[For the Commission

On behalf of the President

[Position]

ANNEX

STOR template

SECTION 1 — IDENTITY OF ENTITY/PERSON SUBMITTING THE STOR Persons professionally arranging or executing transactions in crypto assets — Specify in each case:	
Name of the natural person	[First name(s) and surname(s) of the natural person in charge of the submission of the STOR within the submitting entity.]
Position within the reporting entity	[Position of the natural person in charge of the submission of the STOR within the submitting entity.]
Name of the reporting entity	[Full name of the reporting entity, including for legal persons: — the legal form as provided for in the register of the country pursuant to the law of which it is incorporated, where applicable, and — the Legal Entity Identifier (LEI) code in accordance with ISO 17442 LEI code, where applicable.]
Address of the reporting entity	[Full address (e.g. street, street number, postal code, city, state/province) and country.]
Acting capacity of entity with respect to the orders, transactions or behaviour related to the functioning of the distributed ledger technology that could constitute market abuse	[Description of the capacity in which the reporting entity was acting with regards to the order(s), transaction(s) or behaviour(s) related to the functioning of the distributed ledger technology that could indicate the existence of market abuse, e.g. executing orders on behalf of clients, dealing on own account, operating a trading platform...]
Type of trading activity (market making, arbitrage etc.) and type of crypto-asset traded by the reporting entity	[Description of any corporate, contractual or organisational arrangements or circumstances or relationships, if available]
Contact for additional request for information	Person to be contacted within the reporting entity for additional request for information relating to this report (e.g. compliance officer) and relevant contact details:

	— first name(s) and surname(s), — position of the contact person within the reporting entity, — professional e-mail address.]
SECTION 2 — TRANSACTION/ORDER/BEHAVIOUR AND OTHER ASPECTS RELATED TO THE FUNCTIONING OF THE DISTRIBUTED LEDGER TECHNOLOGY	
Description of the crypto-asset:	Describe the crypto-asset(s) which is the subject of the STOR, specifying: — the full name (including Digital Token Identifier (DTI) in accordance with ISO 24165-2, where applicable) or description of the crypto-asset in the absence of DTI, — the type of crypto-asset (asset-referenced token (ART), e-money token (EMT), other crypto-asset) and for ARTs and EMTs, the value, right or official currency (or combination thereof) which the crypto-asset references in order to maintain a stable value. If the suspicious behaviour involves a trading pair, please list both crypto-assets in the pair.
Description of the distributed ledger (where the STOR refers to the functioning of the distributed ledger technology):	[Describe the distributed ledger, which is the subject of the STOR, specifying the full name and type of the underlying distributed ledger technology
Date and time of transactions, orders or behaviour related to functioning of the distributed ledger technology that could indicate the existence of market abuse	[Indicate the date(s) and time(s) of the order(s), transaction(s) or behaviour(s). Dates and times should be reported in UTC per the format in ISO 8601.]
Trading platform where order was placed or the transaction was executed	[Specify name and Market Identifier Code (MIC) in accordance with ISO 10383 to identify the trading platform where the order was placed or the transaction was executed. If the order/transaction was not identified in a trading platform, please mention ‘outside a trading platform’ and

	the LEI of the CASP(s) that carried out the transaction if applicable.]
Location (country)	[Full name of the country and the ISO 3166-1 two-character country code.] [Specify: — where the order is given (if available), — where the order is executed, — where the behaviour related to functioning of the distributed ledger technology takes place (if available).]
Description of the order, transaction or suspicious behaviour related to the functioning of the distributed ledger technology	[Describe at least the following characteristics of the order(s) or the transaction(s) reported — transaction reference number/order; reference number (where applicable), — settlement date and time, — purchase price/sale price, — volume/quantity of crypto-assets, [Where there are multiple orders or transactions that could constitute market abuse the details on the prices and volumes of such orders and transactions can be provided to the competent authority in an Annex to the STOR.] — information on the order submission, including at least the following: — type of order (e.g. 'buy with limit EUR x'), — the way the order was placed, — the person that actually received the order, — the means by which the order is transmitted. — Information on the order cancellation or alteration (where applicable) including:

	— the nature of the alteration (e.g. change in price or quantity) and the extent of the alteration, [Where there are multiple orders or transactions that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation, the details on the prices and volumes of such orders and transactions can be provided to the competent authority in an Annex to the STOR.] — the means to alter the order (e.g. via e-mail, phone, etc.). In case of reporting a suspicious behaviour related to the functioning of the distributed ledger, please provide as much detail as possible, including the impact it had on the validation of transactions and the method used to alter the functioning of the distributed ledger (where known)
SECTION 3 — DESCRIPTION OF THE NATURE OF THE SUSPICION	
Nature of the suspicion	[Specify the type of breach the reported order(s), transaction(s), behaviour related to the functioning of the distributed ledger functioning, could constitute market abuse].
Reasons for the suspicion	[Description of the activity (transactions and orders, way of placing the orders or executing the transaction and characteristics of the orders and transactions that make them suspicious, behaviours related to the functioning of the distributed ledger functioning) and how the matter came to the attention of the reporting person and specify the reasons for suspicion. For crypto-assets admitted to trading on/traded on a trading platform, a description of the nature of the order book interaction/transactions that could constitute market abuse.]
SECTION 4 — IDENTIFICATION OF PERSON(S) RESPONSIBLE FOR THE ORDERS, TRANSACTIONS OR BEHAVIOUR RELATED TO THE FUNCTIONING OF THE DISTRIBUTED LEDGER TECHNOLOGY THAT COULD CONSTITUTE MARKET ABUSE (‘SUSPECTED PERSON’)	

Name (where applicable and where known)	[For natural persons: the first name(s) and the last name(s).] [For legal persons: full name including legal form as provided for in the register of the country pursuant to the laws of which it is incorporated, if applicable, and Legal Entity Identifier (LEI) code in accordance with ISO 17442, where applicable.]
National Identification Number (where applicable and where known)	[Where applicable in the concerned Member State.] [Number and/or text]. [If the National Identification Number is not applicable or known, provide a date of birth (for natural persons only)] [yyy-mm-dd]
Address (where applicable and where known)	[Full address (e.g. street, street number, postal code, city, state/province) and country.]
Information about the employment: — Place — Position (where applicable and where known)	[Information about the employment of the suspected person, from information sources available internally to the reporting entity (e.g. account documentation in case of clients, staff information system in case of an employee of the reporting entity).]
Account number(s) (where applicable and where known)	[Numbers of the cash and securities account(s), any joint accounts or any Powers of Attorney on the account the suspected entity/person holds.]
Client identifier (where applicable and where known)	[In case the suspected person is a client of the reporting entity.]
Relationship with the issuer of the crypto-asset concerned (where applicable and where known)	[Description of any corporate, contractual or organisational arrangements or circumstances or relationships]
SECTION 5 — ADDITIONAL INFORMATION Background or any other information considered by the reporting entity relevant to the report	
[The following list is not exhaustive. — The position of the suspected person (e.g. retail client, institutions),	

— The nature of the suspected entity's/person's intervention (on own account, on behalf of a client, validator of transactions in a distributed ledger system, other),

— The size of the suspected entity's/person's portfolio,

— The date on which the business relationship with the client started if the suspected entity/person is a client of the reporting person/entity,

— The type of activity of the trading desk, if available, of the suspected entity,

— Trading patterns of the suspected entity/person. For guidance, the following are examples of information that may be useful:

  — trading habits of the suspected entity/person,

  — comparability of the size of the reported order/transaction with the average size of the orders submitted/transactions carried out by the suspected entity/person for the past 12 months,

  — habits of the suspected entity/person in terms of crypto-assets it has traded for the past 12 months, in particular whether the reported order/transaction relates to a crypto-asset which has been traded by the suspected entity/person for the past year.

— Other entities/persons known to be involved in the orders or transactions of which could constitute market abuse:

  — Names,

  — Activity (e.g. executing orders on behalf of clients, dealing on own account, operating a trading platform, validating transactions.)]

SECTION 6 — DOCUMENTATION ATTACHED

[List the supporting attachments and material together provided with this STOR.

Examples of such documentation are e-mails, recordings of conversations, order/transaction records, distributed ledger technology records, confirmations, broker reports, Powers of Attorney documents, and media comment where relevant.

Where the detailed information about the orders/transactions/behaviours related to the functioning of the distributed ledger technology referred to in Section 2 of this template is provided in a separate annex, indicate the title of that annex.]

7.2.2 Draft guidelines on certain aspects of the suitability requirements and format of the periodic statement for portfolio management activities under MiCA

1 Scope

Who?

1. These guidelines apply to competent authorities and crypto-asset service providers, as defined in Article 3(1) (15) of MiCA, where they provide, as relevant, advice on crypto-assets or portfolio management of crypto-assets.

What?

2. These guidelines apply in relation to:

   (i) the suitability requirements under Article 81(1), (7), (8), (10), (11) and (12) of MiCA; and

   (ii) the requirements applicable to the format of the periodic statement to be provided by CASPs providing portfolio management of crypto-assets, in accordance with Article 81(14) of MiCA.

When?

3. These guidelines apply as of [dd mm yyyy].

2 Legislative references, abbreviations and definitions

2.1 Legislative references

ESMA Regulation	Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC[25]
MiCA	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) 1095/2010 and Directives 2013/36/EU and (EU0 2019/1937.

2.2 Abbreviations

ESFS	European System of Financial Supervision
ESMA	European Securities and Markets Authority
EU	European Union

2.3 Definitions

Suitability assessment	The whole process of collecting information about a client and the subsequent assessment by the crypto-asset service provider that a given crypto-asset is suitable for him, based also on the crypto-asset service provider's solid understanding of the crypto-assets that it can recommend or invest into on behalf of the client.
Robo-advice	The provision of advice on crypto-assets or portfolio management of crypto-assets (in whole or in part) through an automated or semi-automated system used as a client-facing tool.

[25] OJ L 331, 15.12.2010, p. 84.

3 Purpose

4. These guidelines are based on Article 81(15) of MiCA and Article 16(1) of the ESMA Regulation. The objectives of these guidelines are to establish consistent, efficient and effective supervisory practices within the ESFS and to ensure the common, uniform and consistent application of the provisions in 81(1), (7), (8), (10), (11), (12) and (14) of MiCA, as relevant.

5. In particular, they aim to promote greater convergence in the application of, and supervisory approaches to, the MiCA suitability requirements and requirements applicable to the format of the periodic statement to be provided by crypto-asset service providers providing portfolio management of crypto-assets.

6. By emphasising a number of important issues and thereby helping to ensure that crypto-asset service providers comply with regulatory standards, ESMA anticipates a corresponding strengthening of investor protection.

4 Compliance and reporting obligations

4.1 Status of the guidelines

7. In accordance with Article 16(3) of the ESMA Regulation, competent authorities and financial market participants must make every effort to comply with these guidelines.

8. Competent authorities to which these guidelines apply should comply by incorporating them into their national legal and/or supervisory frameworks as appropriate, including where particular guidelines are directed primarily at financial market participants. In this case, competent authorities should ensure through their supervision that financial market participants comply with the guidelines.

4.2 Reporting requirements

9. Within two months of the date of publication of the guidelines on ESMA's website in all EU official languages, competent authorities to which these guidelines apply must notify ESMA whether they (i) comply, (ii) do not comply, but intend to comply, or (iii) do not comply and do not intend to comply with the guidelines.

10. In case of non-compliance, competent authorities must also notify ESMA within two months of the date of publication of the guidelines on ESMA's website in all EU official languages of their reasons for not complying with the guidelines.

11. A template for notifications is available on ESMA's website. Once the template has been filled in, it shall be transmitted to ESMA.

12. Financial market participants are not required to report whether they comply with these guidelines.

5 Guidelines on certain aspects of the suitability requirements under MiCA

5.1 Information to clients about the purpose of the suitability assessment and its scope (Guideline 1)

Relevant legislation: Article 66(1) and (2) and 81(1), (8), (10) and (11) of MiCA.

13. Crypto-asset service providers should inform their clients clearly and simply about the suitability assessment and its purpose which is to enable the crypto-asset service provider to act in the client's best interest. This should include a clear explanation that it is the crypto-asset service provider's responsibility to conduct the assessment, so that clients understand (i) the reason why they are asked to provide certain information, (ii) the importance that such information is up-to-date, accurate and complete and (iii) without such information, the crypto-asset service provider will not recommend crypto-asset services or crypto-assets, nor begin the provision of portfolio management of crypto-assets. Such information may be provided in a standardised format.

14. Information about the suitability assessment should help clients understand the purpose of the requirements. It should encourage them to provide up-to-date, accurate and sufficient information about their knowledge, experience, investment objectives (including their risk tolerance) and financial situation (including their ability to bear losses). Crypto-asset service providers should highlight to their clients that it is important to gather complete and accurate information so that the crypto-asset service provider can recommend suitable crypto-assets or crypto-asset services to the client. Without this information, crypto-asset service providers cannot provide advice on crypto-assets or portfolio management of crypto-assets.

15. It is up to the crypto-asset service provider to decide how they will inform their clients about the suitability assessment. The format used should however enable controls to check if the information was provided.

16. Crypto-asset service providers should not create any ambiguity or confusion about their responsibilities in the process when assessing the suitability of crypto-asset services or crypto-assets. Notably, crypto-asset service provider should avoid stating, or giving the impression, that it is the client who decides on the suitability of the investment, or that it is the client who establishes which crypto-assets or crypto-asset services fit his own risk profile. For example, crypto-asset service providers should avoid indicating to the client that a certain crypto-asset is the one that the client chose as being suitable, or requiring the client to confirm that a crypto-asset or crypto-asset service is suitable.

17. Any disclaimers (or other similar types of statements) aimed at limiting the crypto-asset service provider's responsibility for the suitability assessment would not in any way impact the characterisation of the crypto-asset service provided in practice to clients nor the assessment of the crypto-asset service provider's compliance to the corresponding requirements. For example, when collecting clients' information required to conduct a suitability assessment (such as their investment horizon/holding period or information

related to risk tolerance), crypto-asset service providers should not claim that they do not assess the suitability.

18. In order to address potential gaps in clients' understanding of the crypto-asset services provided through robo-advice, crypto-asset service providers should inform clients, in addition to other required information, on the following:

- a very clear explanation of the exact degree and extent of human involvement and if and how the client can ask for human interaction;
- an explanation that the answers clients provide will have a direct impact in determining the suitability of the investment decisions recommended or undertaken on their behalf;
- a description of the sources of information used to generate an investment advice or to provide the portfolio management service (e.g., if an online questionnaire is used, crypto-asset service providers should explain that the responses to the questionnaire may be the sole basis for the robo-advice or whether the crypto-asset service provider has access to other client information or accounts);
- an explanation of how and when the client's information will be updated with regard to his/her situation, personal circumstances, etc.

19. Crypto-asset service providers should also carefully consider whether their disclosures are designed to be effective (e.g., the disclosures are made available directly to clients and are not hidden or incomprehensible). For crypto-asset service providers providing robo-advice this may in particular include:

- emphasising the relevant information (e.g., through the use of design features such as pop-up boxes);
- considering whether some information should be accompanied by interactive text (e.g., through the use of design features such as tooltips) or other means to provide additional details to clients who are seeking further information (e.g., through F.A.Q. section).

5.2 Arrangements necessary to understand clients (Guideline 2)

Relevant legislation: Article 81(1), (8) and (10) of MiCA.

20. Where collecting the information necessary to conduct a suitability assessment for each client, crypto-asset service providers should ensure that the questions they ask their clients are specific enough, are likely to be understood correctly, take into account the elements developed in guideline 3 and that any method used to collect information is designed to get the information required for a suitability assessment.

21. Crypto-asset service providers should ensure that the assessment of information collected about their clients is done in a consistent way irrespective of the means used to collect such information.

22. For example, crypto-asset service providers could use questionnaires (notably in a digital format) completed by their clients, information collected during discussions with them or other information already gathered through the crypto-asset service provider's existing relationship with the client. For instance, a payment default on other obligations may indicate a difficult financial situation.

23. When designing the questionnaires aiming at collecting information about their clients for the purpose of a suitability assessment, crypto-asset service providers should be aware and consider the most common reasons why clients could fail to answer questionnaires correctly. In particular:

- attention should be given to the clarity, exhaustiveness and comprehensibility of the questionnaire, avoiding misleading, confusing, imprecise and excessively technical language;
- the layout should be carefully elaborated and should avoid orienting clients' choices (font, line spacing…);
- presenting questions in batteries (collecting information on a series of items through a single question, particularly when assessing knowledge and experience and the risk tolerance) should be avoided;
- crypto-asset service providers should carefully consider the order in which they ask questions in order to collect information in an effective manner.
- in order to be able to ensure necessary information is collected, the possibility not to reply should generally not be available in questionnaires (particularly when collecting information on the client's financial situation).

24. Crypto-asset service providers should also take reasonable steps to assess the client's understanding of investment risk as well as the relationship between risk and return on investments, as this is key to enable crypto-asset service providers to act in accordance with the client's best interest when conducting the suitability assessment. When presenting questions in this regard, crypto-asset service providers should explain clearly and simply that the purpose of answering them is to help assess clients' attitude to risk (risk profile), and therefore whether crypto-assets are suitable for them (and, if suitable, which types and risks are attached to them).

25. Information necessary to conduct a suitability assessment includes different elements that may affect, for example, the analysis of the client's financial situation (including his ability to bear losses) or investment objectives (including his risk tolerance). Examples of such elements are the client's:

- marital status (especially the client's legal capacity to commit assets that may belong also to his partner);

- family situation (changes in the family situation of a client may impact his financial situation e.g. a new child or a child of an age to start university);

- age (which is mostly important to ensure a correct assessment of the investment objectives, and in particular the level of financial risk that the client is willing to take, as well as the holding period/investment horizon, which indicates the willingness to hold an investment for a certain period of time);

- employment situation (the degree of job security or the fact that the client is close to retirement may impact his financial situation or his investment objectives);

- need for liquidity in certain relevant investments or need to fund a future financial commitment (e.g. property purchase, education fees).

26. When determining what information is necessary, crypto-asset service providers should keep in mind the impact that any significant change regarding that information could have concerning the suitability assessment.

27. ESMA considers it would be a good practice for crypto-asset service providers to consider non-financial elements when gathering information on the client's investment objectives, and – beyond the elements listed in paragraph 25 – collect information on the client's preferences on environmental, social and governance factors in order to take them into account into the suitability assessment.

28. Crypto-asset service providers should take all reasonable steps to sufficiently assess the understanding by their clients of the main characteristics and the risks related to the product types in the offer of the crypto-asset service provider. The adoption by crypto-asset service providers of mechanisms to avoid unduly relying on client's self-assessment and ensure the consistency of the answers provided by the client[26] is particularly important for the correct assessment of the client's knowledge and experience. Information collected by crypto-asset service providers about a client's knowledge and experience should be considered altogether for the overall appraisal of his understanding of the products and of the risks involved in the transactions recommended or in the management of his portfolio.

29. It is also important that crypto-asset service providers appraise the client's understanding of basic financial notions such as investment risk (including concentration risk) and risk-return trade off. To this end, crypto-asset service providers should consider using indicative, comprehensible examples of the levels of loss/return that may arise

[26] See guideline 4.

depending on the level of risk taken and should assess the client's response to such scenarios.

30. As part of the assessment of a client's knowledge and experience, crypto-asset service providers should ensure that the client understands crypto-assets specifically and, in particular, the risks inherent to the use of distributed ledger technology (for instance, cybertheft, hacks, loss or destruction of private keys), on which crypto-assets are based.

31. Crypto-asset service providers should design their questionnaires so that they are able to gather the necessary information about their client. This is particularly relevant for crypto-asset service providers providing robo-advice services given the limited human interaction. In order to ensure their compliance with the requirements concerning that assessment, crypto-asset service providers should take into account factors such as:

- whether the information collected through the online questionnaire allows the crypto-asset service provider to conclude that the advice provided is suitable for their clients on the basis of their knowledge and experience, their financial situation and their investment objectives and needs;
- whether the questions in the questionnaire are sufficiently clear and/or whether the questionnaire is designed to provide additional clarification or examples to clients when necessary (e.g., through the use of design features, such as tool-tips or pop-up boxes);
- whether some human interaction (including remote interaction via emails or mobile phones) is available to clients when responding to the online questionnaire;
- whether steps have been taken to address inconsistent client responses (such as incorporating in the questionnaire design features to alert clients when their responses appear internally inconsistent and suggest them to reconsider such responses; or implementing systems to automatically flag apparently inconsistent information provided by a client for review or follow-up by the crypto-asset service provider).

5.3 Extent of information to be collected from clients (proportionality) (Guideline 3)

Relevant legislation: Article 81(1), (8) and (10) of MiCA

32. Before providing advice on crypto-assets or portfolio management of crypto-assets, crypto-asset service providers need to collect all 'necessary information'[27] about the client's knowledge and experience, financial situation, investment objectives and their basic understanding of the risks involved in purchasing crypto-assets. The extent of 'necessary' information may vary and crypto-asset service providers should determine

[27] 'Necessary information' should be understood as meaning the information that crypto-asset service providers must collect to comply with the suitability requirements under MiCA.

the extent of the information to be collected from clients in light of all the features of the advice on crypto-assets or portfolio management of crypto-assets to be provided to those clients. Notably, crypto-asset service providers should take into account the features of the advice on crypto-assets or portfolio management of crypto-assets to be provided, the type and characteristics of the crypto-assets to be considered and the characteristics of the clients.

33. Crypto-asset service providers should obtain from clients or potential clients such information as is necessary for the crypto-asset service provider to understand essential facts about the client and to have a reasonable basis for determining, giving due consideration to the nature and extent of the service provided, that the specific transaction to be recommended, or entered into the course of providing portfolio management of crypto-assets, satisfies the following criteria:

- it meets the investment objectives of the client in question, including client's risk tolerance;
- it is such that the client is able financially to bear any related investment risks consistent with his investment objectives;
- it is such that the client has the necessary experience and knowledge in order to understand the risks involved in the transaction or in the management of his portfolio.

34. In determining what information is 'necessary', crypto-asset service providers should consider, in relation to a client's knowledge and experience, financial situation, investment objectives and their basic understanding of the risks involved in purchasing crypto-assets:

- the type of crypto-assets or transactions that the crypto-asset service provider may recommend or enter into (including the complexity and level of risk);
- the nature and extent of the service that the crypto-asset service provider may provide;
- the needs and circumstances of the client;
- the features of the client (e.g., their level of sophistication, knowledge of investing (including in relation to crypto-assets), financial situation…).

35. Crypto-asset service providers should ensure that the information regarding a client's or potential client's knowledge and experience in investing, including in the crypto-asset field, includes the following, to the extent appropriate to the nature of the client, the nature and extent of the service to be provided and the type of crypto-asset or transaction envisaged, including their complexity and the risks involved:

- the types of service, transaction and financial products with which the client is familiar;
- whether the client understands distributed ledger technology, on which crypto-assets are based, and the risks inherent to it;
- the nature, volume, and frequency of the client's transactions, including in crypto-assets, and the period over which they have been carried out;
- the level of education, and profession or relevant former profession of the client or potential client.

36. When assessing a client's knowledge of crypto-assets or a particular type of crypto-assets, crypto-asset service providers should not solely rely on such client's transaction history but should ensure the client's understanding of the product.

37. While the extent of the information to be collected may vary, the standard for ensuring that a recommendation or an investment made on the client's behalf is suitable for the client will always remain the same. MiCA allows crypto-asset service providers to collect the level of information that is adequate for and proportionate to the products and services they offer, or on which the client requests specific advice on crypto-assets or portfolio management of crypto-assets. It does not allow crypto-asset service providers to lower the level of protection due to clients.

38. The information regarding the investment objectives of the client or potential client should include, where relevant, information on the length of time for which the client wishes to hold the investment, his or her preferences regarding risk taking, his or her risk profile, and the purposes of the investment.

39. For such risky and complex products as crypto-assets, crypto-asset service providers should collect more in-depth information about the client than they would collect when less complex or risky products are at stake. This is so that crypto-asset service providers can assess the client's capacity to understand, and financially bear, the risks associated with crypto-assets.[28] ESMA expects crypto-asset service providers to carry out a robust assessment amongst others of the client's knowledge and experience, including, for example, the ability to understand the mechanisms which make crypto-assets in general and the specific type of crypto-asset recommended or traded "risky" and, possibly, "complex", whether the client has already traded in crypto-assets and the specific type of crypto-assets (for example, a stablecoin or a utility token), the length of time he has been trading them for, etc.

[28] To ensure clients understand the investment risk and potential losses they may bear, the crypto-asset service provider should, as far as possible, present these risks in a clear and understandable way, potentially using illustrative examples of the extent of losses in the event of a crypto-asset performing poorly.

40. For illiquid crypto-assets[29], the 'necessary information' to be gathered should include information on the length of time for which the client is prepared to hold the investment.

41. As information about a client's financial situation will always need to be collected, the extent of information to be collected may depend on the type of crypto-assets to be recommended or entered into. For example, as all crypto-assets are highly speculative investments, 'necessary information' to be collected may include all of the following elements as necessary to ensure whether the client's financial situation allows him to invest or be invested in such crypto-assets:

- the extent of the client's regular income and total income, whether the income is earned on a permanent or temporary basis, and the source of this income (for example, from employment, retirement income, investment income, rental yields, etc.);

- the client's assets, including liquid assets, investments and real property, which would include what financial investments, personal and investment property, pension funds and any cash deposits, etc. the client may have. The crypto-asset service provider should, where relevant, also gather information about conditions, terms, access, loans, guarantees and other restrictions, if applicable, to the above assets that may exist.

- the client's regular financial commitments, which would include what financial commitments the client has made or is planning to make (client's debits, total amount of indebtedness and other periodic commitments, etc.).

42. In determining the information to be collected, crypto-asset service providers should also take into account the nature of the service to be provided. Practically, this means that:

- when advice on crypto-assets is to be provided, crypto-asset service providers should collect sufficient information in order to be able to assess the ability of the client to understand the risks and nature of each of the crypto-assets that the crypto-asset service provider envisages recommending to that client, as well as the mechanisms which make crypto-assets in general and the specific type of crypto-asset recommended "risky" and "complex";

- when portfolio management of crypto-assets is to be provided, as investment decisions are to be made by the crypto-asset service provider on behalf of the client, the level of knowledge and experience needed by the client with regard to all the crypto-assets that can potentially make up the portfolio may be less detailed than the level that the client should have when an advice on crypto-assets service is to be provided. Nevertheless, even in such situations, the client should at least understand the overall risks of the portfolio (including the risks inherent to

[29] It is up to each crypto-asset service provider to define a priori which of the crypto-assets included in its offer to investors it considers as being illiquid.

distributed ledger technology) and possess a general understanding of the risks linked to each type of crypto-assets that can be included in the portfolio. Crypto-asset service providers should gain a very clear understanding and knowledge of the degree of understanding of crypto-assets and of the investment profile of the client.

43. Similarly, the extent of the service requested by the client may also impact the level of detail of information collected about the client. For example, crypto-asset service providers should collect more information about clients asking for advice covering their entire financial portfolio than about clients asking for specific advice on how to invest a given amount of money that represents a relatively small part of their overall portfolio.

44. Crypto-asset service providers should also take into account the nature of the client when determining the information to be collected. For example, more in-depth information would usually need to be collected for potentially vulnerable clients (such as older clients could be) or inexperienced ones asking for advice on crypto-assets or portfolio management of crypto-asset services for the first time.

45. Information to be collected will also depend on the needs and circumstances of the client. For example, a crypto-asset service provider is likely to need more detailed information about the client's financial situation where the client's investment objectives are multiple and/or long-term, than when the client seeks a short-term investment.

46. Information about a client's financial situation includes information regarding his or her investments (in crypto-assets and other products). This implies that crypto-asset service providers are expected to possess information about the client's financial investments he holds with the crypto-asset service provider on a crypto-asset by crypto-asset basis. Depending on the scope of advice provided, crypto-asset service providers should also encourage clients to disclose details on investments they hold with other crypto-asset service providers or financial investments they hold with financial institutions, if possible also on a product-by-product basis.

5.4 Reliability of client information (Guideline 4)

Relevant legislation: Article 81(1) and (10) of MiCA.

47. Clients are expected to provide correct, up-to-date and complete information necessary for the suitability assessment. However, crypto-asset service providers should take all reasonable steps and have appropriate tools to ensure that the information collected about their clients is reliable, accurate and consistent, without unduly relying on clients' self-assessment. This should include, without limitation:

- ensuring clients are aware of the importance of providing accurate and up-to-date information;

- ensuring all tools, such as risk assessment profiling tools or tools to assess a client's knowledge and experience, employed in the suitability assessment process are fit-for-purpose and are appropriately designed for use with their clients, with any limitations identified and actively mitigated through the suitability assessment process;

- ensuring questions used in the process are likely to be understood by clients, capture an accurate reflection of the client's objectives and needs, and the information necessary to understand the suitability assessment; and

- taking steps, as appropriate, to ensure the consistency of client information, such as by considering whether there are obvious inaccuracies in the information provided by clients.

48. Crypto-asset service providers remain responsible for ensuring they have the necessary information to conduct a suitability assessment. In this respect, any agreement signed by the client, or disclosure made by the crypto-asset service provider, that would aim at limiting the responsibility of the crypto-asset service provider with regard to the suitability assessment, would not be considered compliant with the relevant requirements in MiCA.

49. To avoid unduly relying on client's self-assessment, any auto-evaluation should be counterbalanced by factual information gathered on the basis of objective criteria. For example:

- instead of asking whether a client understands the notions of risk-return trade-off and risk diversification, the crypto-asset service provider should present some practical examples of situations that may occur in practice, for example by means of graphs or through positive and negative scenarios which are based on reasonable assumptions;

- instead of asking whether a client has sufficient knowledge about the main characteristics and risks of specific types of crypto-assets, the crypto-asset service provider should for instance ask questions aimed at assessing the client's real knowledge about the specific types of crypto-assets, for example by asking the client multiple choice questions to which the client should provide the right answer;

- instead of asking a client whether he feels sufficiently experienced to invest in certain crypto-assets, the crypto-asset service provider should ask the client what types of crypto-assets the client is familiar with and how recent and frequent his trading experience with them is;

- instead of asking whether clients believe they have sufficient funds to invest, the crypto-asset service provider should ask clients to provide factual information about their financial situation, e.g. the regular source of income and whether outstanding liabilities exist (such as bank loans or other debts, which may

significantly impact the assessment of the client's ability to financially bear any risks and losses related to the investment);

- instead of asking whether a client feels comfortable with taking risk, the crypto-asset service provider should ask what level of loss over a given time period the client would be willing to accept, either on the individual investment or on the overall portfolio.

50. In assessing a client's knowledge and experience, a crypto-asset service provider should also avoid using overly broad questions with a yes/no type of answer and or a very broad tick-the-box self-assessment approach (for example, crypto-asset service providers should avoid submitting a list of crypto-assets to the client and asking him/her to indicate which s/he understands). Where crypto-asset service providers pre-fill answers based on the client's transactions history with that crypto-asset service provider (e.g., through another crypto-asset service provided), they should ensure that only fully objective, pertinent, and reliable information is used and that the client is given the opportunity to review and, if necessary, correct and/or complete each of the pre-filled answers to ensure the accuracy of any pre-populated information. Crypto-asset service providers should also refrain from predicting clients' experience based on assumptions.

51. A client's prior investments in crypto-assets should not be sufficient in itself for the crypto-asset service provider to conclude that such client understands crypto-assets and crypto-asset services (especially the risks associated with crypto-assets).

52. When assessing the risk tolerance of their clients through a questionnaire, crypto-asset service providers should not only investigate the desirable risk-return characteristics of future investments but they should also take into account the client's risk perception. To this end, whilst self-assessment for the risk tolerance should be avoided, explicit questions on the clients' personal choices in case of risk uncertainty could be presented. Furthermore, crypto-asset service providers could for example make use of graphs, specific percentages or concrete figures when asking the client how he would react when the value of his portfolio decreases.

53. Where crypto-asset service providers rely on tools to be used by clients as part of the suitability process (such as questionnaires or risk-profiling software), they should ensure that they have appropriate systems and controls to ensure that the tools are fit for purpose and produce satisfactory results. For example, risk-profiling software could include some controls of coherence of the replies provided by clients in order to highlight contradictions between different pieces of information collected.

54. Crypto-asset service providers should also take reasonable steps to mitigate potential risks associated with the use of such tools. For example, potential risks may arise if clients were encouraged to provide certain answers in order to get access to crypto-

assets or crypto-asset services that may not be suitable for them (without correctly reflecting the clients' real circumstances and needs). [30]

55. In order to ensure the consistency of client information, crypto-asset service providers should view the information collected as a whole. Crypto-asset service providers should be alert to any relevant contradictions between different pieces of information collected, and contact the client in order to resolve any material potential inconsistencies or inaccuracies. Examples of such contradictions are clients who have little knowledge or experience and an aggressive attitude to risk, or who have a prudent risk profile and ambitious investment objectives.

56. Crypto-asset service providers should adopt mechanisms to address the risk that clients may tend to overestimate their knowledge and experience, for example by including questions that would help crypto-asset service providers assess the overall clients' understanding about the characteristics and the risks of crypto-assets in general and the different types of crypto-assets. Such measures may be particularly important in the case of robo-advice, since the risk of overestimation by clients may result higher when they provide information through an automated (or semi-automated) system, especially in situations where very limited or no human interaction at all between clients and the crypto-asset service provider's employees is foreseen.

5.5 Updating client information (Guideline 5)

Relevant legislation: Article 81(1), (8), (10) and (12) of MiCA.

57. Where a crypto-asset service provider has an ongoing relationship with the client (such as by providing ongoing advice on crypto-assets or portfolio management of crypto-assets), in order to be able to perform the suitability assessment, crypto-asset service providers should adopt procedures defining: (a) what part of the client information collected should be subject to updating and at which frequency; (b) how the updating should be done and what action should be undertaken by the crypto-asset service provider when additional or updated information is received or when the client fails to provide the information requested.

58. Crypto-asset service providers should regularly review client information to ensure that it does not become manifestly out of date, inaccurate or incomplete. To this end, crypto-asset service providers should implement procedures to encourage clients to update the information originally provided where significant changes occur.

59. Frequency of update might vary depending on, for example, clients' risk profiles and taking into account the type of crypto-asset recommended. Based on the information collected about a client under the suitability requirements, a crypto-asset service provider will determine the client's risk profile, i.e. what type of crypto-asset services or crypto-

[30] In this regard, see also paragraph 60 of guideline 5, which addresses the risk of clients being influenced by crypto-asset service providers to change answers previously provided by them, without there being any real modification in their situation.

assets can in general be suitable for him taking into account his knowledge and experience, his financial situation (including his ability to bear losses) and his investment objectives (including his risk tolerance). For example, a risk profile giving to the client access to a wider range of riskier products is an element that is likely to require more frequent updating. Certain events might also trigger an updating process; this could be so, for example, for clients reaching the age of retirement or facing unemployment.

60. Due to the requirement to review the suitability assessment at least every two years (in accordance with Article 81(12) of MiCA), updates should occur at least every two years to ensure that the updated suitability assessment is not based on outdated client's information. This also implies that the update should be done prior to any new suitability assessment occurring on the two-year deadline.

61. Updating could, for example, be carried out by sending an updating questionnaire to clients. Relevant actions might include changing the client's profile based on the updated information collected.

62. It is also important that crypto-asset service providers adopt measures to mitigate the risk of inducing the client to update his own profile so as to make appear as suitable a certain investment product that would otherwise be unsuitable for him, without there being a real modification in the client's situation.[31] As an example of a good practice to address this type of risk, crypto-asset service providers could adopt procedures to verify, before or after transactions are made, whether a client's profile has been updated too frequently or only after a short period from last modification (especially if this change has occurred in the immediate days preceding a recommended investment). Such situations would therefore be escalated or reported to the relevant control function. These policies and procedures are particularly important in situations where there is a heightened risk that the interest of the crypto-asset service provider may come into conflict with the best interests of its clients, e.g. in situations in which the crypto-asset service provider is placing crypto-assets with its own clients. Another relevant factor to consider in this context is also the type of interaction that occurs with the client (e.g. telephone conversation vs through an automated system).

63. Crypto-asset service providers should inform the client when the additional information provided results in a change of his profile, whether it becomes more risky (and therefore, potentially, a wider range of riskier and more complex crypto-assets may as a result be suitable for him, with the potential to incur in higher losses) or vice-versa more conservative (and therefore, potentially, a more restricted range of crypto-assets may as a result be suitable for him).

5.6 Client information for legal entities or groups (Guideline 6)

[31] Also relevant in this context are measures adopted to ensure the reliability of clients' information as detailed under guideline 4, paragraph 45.

Relevant legislation: Article 81(1), (8) and (10) of MiCA.

64. Where a client is a legal person or a group of two or more natural persons or where one or more natural persons are represented by another natural person, the crypto-asset service provider should establish and implement a policy, on an ex-ante basis, on the procedure and criteria that should be followed in order to comply with the MiCA suitability requirements in such situations. This includes (i) who should be subject to the suitability assessment, (ii) how the suitability assessment should be done in practice, including from whom information about knowledge and experience, financial situation and investment objectives should be collected and (iii) the possible impact this could have for the relevant clients, in accordance with the existing policy.

65. Where a client is a legal person or a natural person represented by another natural person, the financial situation and investment objectives should be assessed in light of those of the underlying client (the legal person or the natural person that is being represented) rather than of the representative. The knowledge and experience to be assessed should be that of the representative. This would imply amongst others that they verify that the representative is indeed – according to relevant national law – authorised to carry out transactions on behalf of the client.

66. Crypto-asset service providers should consider whether the applicable national legal framework provides specific indications that should be taken into account for the purpose of conducting the suitability assessment (this could be the case, for instance, where the appointment of a legal representative is required by law: e.g. for underage or incapacitated persons or for a legal person).

67. The policy should make a clear distinction between situations where a representative is foreseen under applicable national law, as it can be the case for example for legal persons, and situations where no representative is foreseen, and it should focus on these latter situations. Where the policy foresees agreements between clients, they should be made aware clearly and in written form about the effects that such agreements may have regarding the protection of their respective interests. Steps taken by the crypto-asset service provider in accordance with its policy should be appropriately documented to enable ex-post controls.

68. Where the client is a group of two or more natural persons and no representative is foreseen under applicable national law, the crypto-asset service provider's policy should identify from whom necessary information will be collected and how the suitability assessment will be done. Clients should be properly informed about the crypto-asset service provider's approach (as decided in its policy) and the impact of this approach on the way the suitability assessment is done in practice.

69. Approaches such as the following could possibly be considered by crypto-asset service providers: (a) they could choose to invite the group of two or more natural persons to designate a representative; or, (b) they could consider collecting information about each individual client and assessing the suitability for each individual client.

Inviting the group of two or more natural persons to designate a representative

70. If the group of two or more natural persons agrees to designate a representative, the same approach as the one described in paragraph 65 above could be followed: the knowledge and experience shall be that of the representative, while the financial situation and the investment objectives would be those of the underlying client(s). Such designation should be made in written form as well as according to and in compliance with the applicable national law, and recorded by the relevant crypto-asset service provider. The clients - part of the group - should be clearly informed, in written form, about the impact that an agreement amongst clients could have on the protection of their respective interests.

71. The crypto-asset service provider's policy could however require the underlying client(s) to agree on their investment objectives.

72. If the parties involved have difficulties in deciding the person/s from whom the information on knowledge and experience should be collected, the basis on which the financial situation should be determined for the purpose of the suitability assessment or on defining their investment objectives, the crypto-asset service provider should adopt the most prudent approach by taking into account, accordingly, the information on the person with the least knowledge and experience, the weakest financial situation or the most conservative investment objectives. Alternatively, the crypto-asset service provider's policy may also specify that it will not be able to provide advice on crypto-assets or portfolio management of crypto-assets in such a situation. Crypto-asset service providers should at least be prudent whenever there is a significant difference in the level of knowledge and experience or in the financial situation of the different clients part of the group.

Collecting information about each individual client and assessing the suitability for each individual client

73. When a crypto-asset service provider decides to collect information and assess suitability for each individual client part of the group, if there are significant differences between the characteristics of those individual clients (for example, if the crypto-asset service provider would classify them under different investment profiles), the question arises about how to ensure the consistency of the advice on crypto-assets or portfolio management of crypto-assets provided with regard to the crypto-assets or portfolio of that group of clients. In such a situation, a crypto-asset may be suitable for one client part of the group but not for another one. The crypto-asset service provider's policy should clearly specify how it will deal with such situations. Here again, the crypto-asset service provider should adopt the most prudent approach by taking into account the information on the client part of the group with the least knowledge and experience, the weakest financial situation or the most conservative investment objectives. Alternatively, the crypto-asset service provider's policy may also specify that it will not be able to provide advice on crypto-assets or portfolio management of crypto-assets in such a situation. In this context, it should be noted that collecting information on all the clients

part of the group and considering, for the purposes of the assessment, an average profile of the level of knowledge and competence of all of them, would unlikely be compliant with the MiCA overarching principle of acting in the clients' best interests.

5.7 Arrangements necessary to understand crypto-assets (Guideline 7)

Relevant legislation: Article 81(10) of MiCA.

74. Crypto-asset service providers should have adequate policies and procedures in place to ensure that they understand the characteristics, nature, features, including costs and risks of crypto-asset services and crypto-assets selected for their clients and that they assess, while taking into account cost and complexity, whether equivalent crypto-asset services or crypto-assets can meet their client's profile.

75. Crypto-asset service providers should adopt robust and objective procedures, methodologies and tools that allow them to appropriately consider the different characteristics and relevant risk factors (such as credit risk, market risk, liquidity risk[32], operational risk including hacking risk, etc.) of each crypto-asset they may recommend or invest in on behalf of clients. Considering the level of 'complexity' of products is particularly important, and this should be matched with a client's information (in particular regarding their knowledge and experience).

76. Crypto-asset service providers should adopt procedures to ensure that the information used to understand and correctly classify crypto-assets included in their product offer is reliable, accurate, consistent and up-to-date. When adopting such procedures, crypto-asset service providers should take into account the different characteristics and nature of the crypto-assets considered.

77. In addition, crypto-asset service providers should review the information used so as to be able to reflect any relevant changes that may impact the product's classification. This is particularly important, taking into account the continuing evolution and growing speed of crypto-asset markets.

5.8 Arrangements necessary to ensure the suitability of crypto-assets or crypto-asset services (Guideline 8)

Relevant legislation: Articles 68(4) and 81(1), (10), (11) and (12) of MiCA.

78. In order to match clients with suitable investments, crypto-asset service providers should establish policies and procedures to ensure that they consistently take into account:

[32] It is particularly important that the liquidity risk identified is not balanced out with other risk indicators (such as, for example, those adopted for the assessment of credit/counterparty risk and market risk). This is because the liquidity features of crypto-assets should be compared with information on the client's willingness to hold the crypto-assets for a certain length of time, i.e. the so called 'holding period'.

- all available information about the client necessary to assess whether a crypto-asset is suitable, including the client's current portfolio of investments (and asset allocation within that portfolio which should not be limited to crypto assets allocation);

- all material characteristics of the crypto-assets considered in the suitability assessment, including all relevant risks and any direct or indirect costs to the client.

79. Crypto-asset service providers are reminded that the suitability assessment is not limited to recommendations to buy a crypto-asset. Every recommendation must be suitable, whether it is, for example, a recommendation to buy, hold or sell a crypto-asset, or not to do so.

80. Crypto-asset service providers that rely on tools in the suitability assessment process (such as model portfolios, asset allocation software or a risk-profiling tool for potential investments), should have appropriate systems and controls to ensure that the tools are fit for purpose and produce satisfactory results.

81. In this regard, the tools should be designed so that they take account of all the relevant specificities of each client or crypto-asset. For example, tools that classify clients or crypto-assets broadly would not be fit for purpose.

82. A crypto-asset service provider should establish policies and procedures which enable it to ensure inter alia that:

- the advice on crypto-assets and portfolio management of crypto-assets services provided to the client take account of an appropriate degree of risk diversification, including regarding the type of instruments held in the portfolio (crypto assets, financial instruments, etc.);

- the client has an adequate understanding of the relationship between risk and return, i.e. of the necessarily low remuneration of risk free assets, of the incidence of time horizon on this relationship and of the impact of costs on his investments;

- the financial situation of the client can finance the crypto-assets and the client can bear any possible losses resulting from the investments;

- any personal recommendation or transaction entered into in the course of providing advice on crypto-assets or portfolio management of crypto-assets, where an illiquid product is involved, takes into account the length of time for which the client is prepared to hold the investment; and

- any conflicts of interest are prevented from adversely affecting the quality of the suitability assessment.

83. When making a decision on the methodology to be adopted to conduct the suitability assessment, the crypto-asset service provider should also take into account the type and

characteristics of the crypto-asset services provided and, more in general, its business model.

84. When conducting a suitability assessment, a crypto-asset service provider providing the service of portfolio management of crypto-assets should, on the one hand, assess - in accordance with the second bullet point of paragraph 42 of these guidelines - the knowledge and experience of the client regarding each type of crypto-asset that could be included in his portfolio, and the types of risks involved in the management of his portfolio. Depending on the level of complexity of the crypto-assets involved, the crypto-asset service provider should assess the client's knowledge and experience more specifically than solely on the basis of the type to which the crypto-asset belongs. On the other hand, with regard to the client's financial situation and investment objectives, the suitability assessment about the impact of the crypto-asset(s) and transaction(s) can be done at the level of the client's portfolio as a whole. In practice, if the portfolio management agreement defines in sufficient details the investment strategy that is suitable for the client with regard to the suitability criteria defined by MiCA and that will be followed by the crypto-asset service provider, the assessment of the suitability of the investment decisions could be done against the investment strategy as defined in the portfolio management agreement and the portfolio of the client as a whole should reflect this agreed investment strategy. When a crypto-asset service provider conducts a suitability assessment based on the consideration of the client's portfolio as a whole within the service of advice on crypto-assets, this means that, on the one hand, the level of knowledge and experience of the client should be assessed regarding each crypto-asset and risks involved in the related transaction. On the other hand, with regard to the client's financial situation and investment objectives, the suitability assessment about the impact of the product and transaction can be done at the level of the client's portfolio.

85. When a crypto-asset service provider conducts a suitability assessment based on the consideration of the client's portfolio as a whole, it should ensure an appropriate degree of diversification within the client's portfolio, taking into account the client's portfolio exposure to the different financial risks (geographical exposure, currency exposure, etc.). Crypto-asset service providers should be especially prudent regarding credit risk: exposure of the client's portfolio to one single issuer or to issuers part of the same group should be particularly considered. This is because, if a client's portfolio is concentrated in products issued by one single entity (or entities of the same group), in case of default of that entity, the client may lose up to his entire investment.

86. In order to ensure the consistency of the suitability assessment conducted through automated tools (even if the interaction with clients does not occur through automated systems), crypto-asset service providers should regularly monitor and test the algorithms that underpin the suitability of the transactions recommended or undertaken on behalf of clients. When defining such algorithms, crypto-asset service providers should take into account the nature and characteristics of the crypto-assets included in their offer to clients. In particular, crypto-asset service providers should at least:

- establish an appropriate system-design documentation that clearly sets out the purpose, scope and design of the algorithms. Decision trees or decision rules should form part of this documentation, where relevant;

- have a documented test strategy that explains the scope of testing of algorithms. This should include test plans, test cases, test results, defect resolution (if relevant), and final test results;

- have in place appropriate policies and procedures for managing any changes to an algorithm, including monitoring and keeping records of any such changes. This includes having security arrangements in place to monitor and prevent unauthorised access to the algorithm;

- review and update algorithms to ensure that they reflect any relevant changes (e.g. market changes and changes in the applicable law) that may affect their effectiveness;

- have in place policies and procedures enabling to detect any error within the algorithm and deal with it appropriately, including, for example, suspending the provision of advice if that error is likely to result in an unsuitable advice and/or a breach of relevant law/regulation;

- have in place adequate resources, including human and technological resources, to monitor and supervise the performance of algorithms through an adequate and timely review of the advice provided; and

- have in place an appropriate internal sign-off process to ensure that the steps above have been followed.

87. Where advice on crypto-assets or portfolio management of crypto-assets are provided in whole or in part through an automated or semi-automated system, the responsibility to undertake the suitability assessment should remain with the crypto-asset service provider providing the service and shall not be reduced by the use of an electronic system in making the personal recommendation or decision to trade.

5.9 Costs and complexity of equivalent products (Guideline 9)

Relevant legislation: Article 81(1), (10) and (12) of MiCA.

88. Suitability policies and procedures should ensure that, before a crypto-asset service provider makes a decision on the crypto-asset(s) that will be recommended, or invested in the portfolio managed on behalf of the client, a thorough assessment of the possible crypto-assets and crypto-asset services alternatives is undertaken, taking into account products' cost and complexity.

89. A crypto-asset service provider should have a process in place, taking into account the nature of the service, its business model and the type of crypto-assets that are provided,

to assess crypto-assets available that are ‘equivalent’ to each other in terms of ability to meet the client’s needs and circumstances, such as crypto-assets with similar target clients and similar risk-return profile.

90. When considering the cost factor, crypto-asset service providers should take into account all costs and charges covered by the relevant provisions under Article 81(4) of MiCA. As for the complexity, crypto-asset service providers should refer to the criteria identified in the above guideline 7. For crypto-asset service providers with a restricted range of crypto-assets, or those recommending one type of crypto-asset, where the assessment of ‘equivalent’ crypto-asset could be limited, it is important that clients are made fully aware of such circumstances. In this context, it is particularly important that clients are provided appropriate information on how restricted the range of crypto-assets offered is, pursuant to Article 81(2)(b) of MiCA.[33]

91. Where a crypto-asset service provider uses common portfolio strategies or model investment propositions that apply to different clients with the same investment profile (as determined by the crypto-asset service provider), the assessment of cost and complexity for 'equivalent’ crypto-assets could be done on a higher level, centrally, (for example within an investment committee or any other committee defining common portfolio strategies or model investment propositions) although a crypto-asset service provider will still need to ensure that the selected crypto-assets are suitable and meet their clients’ profile on a client-by-client basis.

92. Crypto-asset service providers should be able to justify those situations where a more costly or complex crypto-asset is chosen or recommended over an equivalent crypto-asset, taking into account that for the selection process of products in the context of advice on crypto-assets or portfolio management further criteria can also be considered (for example: the portfolio’s diversification, liquidity, or risk level). Crypto-asset service providers should document and keep records about these decisions, as these decisions should deserve specific attention from control functions within the crypto-asset service provider. The respective documentation should be subject to internal reviews. When providing advice on crypto-assets crypto-asset service providers could, for specific well-defined reasons, also decide to inform the client about the decision to choose the more costly and complex crypto-asset.

5.10 Costs and benefits of switching investments (Guideline 10)

Relevant legislation: Article 81(1), (10) and (12) of MiCA.

93. Crypto-asset service providers should have adequate policies and procedures in place to ensure that an analysis of the costs and benefits of a switch is undertaken such that

[33] In accordance with MiCA, crypto-asset service providers are therefore not expected to consider the whole universe of possible crypto-asset options existing in the market in order to follow guideline 7, paragraph 73.

crypto-asset service providers are reasonably able to demonstrate that the expected benefits of switching are greater than the costs.

94. For the purpose of this guideline, investment decisions such as rebalancing a portfolio under management, in the case of a "passive strategy" to replicate an index (as agreed with the client) would normally not be considered as a switch. For the avoidance of doubt, any transaction without maintaining these thresholds would be considered as a switch.

95. Crypto-asset service providers should take all necessary information into account, so as to be able to conduct a cost-benefit analysis of the switch, i.e. an assessment of the advantages and disadvantages of the new crypto-asset(s) considered. When considering the cost dimension, crypto-asset service providers should take into account all costs and charges covered by the relevant provisions under Article 81(4) of MiCA. In this context, both monetary and non-monetary factors of costs and benefits could be relevant. These may include, for example:

- the expected net return of the proposed alternative transaction (which also considers any possible up-front cost to be paid by the client(s)) vs the expected net return of the existing investment (that should also consider any exit cost which the client(s) might incur to divest from the crypto-asset already in his/their portfolio);
- a change in the client's circumstances and needs, which may be the reason for considering the switch, e.g. the need for liquidity in the short term as a consequence of an unexpected and unplanned family event;
- a change in the crypto-assets' features and/or market circumstances, which may be a reason for considering a switch in the client(s) portfolio(s), e.g. if a crypto-asset becomes illiquid due to market trends;
- benefits to the client's portfolio stemming from the switch, such as (i) an increase in the portfolio diversification (by geographical area, type of crypto-asset, type of issuer, etc.); (ii) an increased alignment of the portfolio's risk profile with the client's risk objectives; (iii) an increase in the portfolio's liquidity; or (iv) a decrease of the overall credit risk of the portfolio.

96. When providing advice on crypto-assets, a clear explanation of whether or not the benefits of the recommended switch are greater than its costs should be included in the suitability report[34] the crypto-asset service provider has to provide to the client before the transaction is made.

97. Crypto-asset service providers should also adopt systems and controls to monitor the risk of circumventing the obligation to assess costs and benefits of recommended switch, for example in situations where an advice to sell a crypto-asset is followed by an advice

[34] The report on suitability referred to in Article 81(13) of MiCA.

to buy another crypto-asset at a later stage (e.g. days later), but the two transactions were in fact strictly related from the beginning.

98. Where a crypto-asset service provider uses common portfolio strategies or model investment propositions that apply to different clients with the same investment profile (as determined by the crypto-asset service provider), the costs/benefits analysis of a switch could be done on a higher level than at the level of each individual client or each individual transaction. More especially, when a switch is decided centrally, for example within an investment committee or any other committee defining common portfolio strategies or model investment propositions, the costs/benefits analysis could be done at the level of that committee. If such a switch is decided centrally, the costs/benefits analysis done at that level would usually be applicable to all comparable client portfolios without making an assessment for each individual client. In such a situation also, the crypto-asset service provider could determine, at the level of the relevant committee, the reason why a switch decided will not be performed for certain clients. Although the costs/benefits analysis could be done at a higher level in such situations, the crypto-asset service provider should nevertheless have appropriate controls in place to check that there are no particular characteristics of certain clients that might require a more discrete level of analysis.

99. Where a portfolio manager has agreed a more bespoke mandate and investment strategy with a client due to the client's specific investment needs, a cost-benefit analysis of the switch at client-level should be more appropriate, in contrast to the above.

100. Notwithstanding the above, if a portfolio manager considers that the composition or parameters of a portfolio should be changed in a way that is not permitted by the mandate agreed with the client, the portfolio manager should discuss this with the client and review or conduct a new suitability assessment to agree a new mandate.

5.11 Qualifications of staff (Guideline 11)

Relevant legislation: Articles 68(5) and 81(7) of MiCA.

101. Crypto-asset service providers are required to ensure that staff involved in material aspects of the suitability process have an adequate level of skills, knowledge and expertise with regard to crypto-assets and crypto-asset services.

102. Staff should understand the role they play in the suitability assessment process and possess the skills, knowledge and expertise necessary, including sufficient knowledge of the relevant regulatory requirements and procedures, to discharge their responsibilities.

103. Staff should possess the necessary knowledge and competence, including with regard to the suitability assessment. To that effect, crypto-asset service providers should give staff appropriate training.

104. Other staff that does not directly face clients but is involved in the suitability assessment in any other way must still possess the necessary skills, knowledge and expertise required depending on their particular role in the suitability process. This may regard, for example, setting up the questionnaires, defining algorithms governing the assessment of suitability or other aspects necessary to conduct the suitability assessment and controlling compliance with the suitability requirements.

105. Where relevant, when employing automated tools (including hybrid tools), crypto-asset service providers should ensure that their staff involved in the activities related to the definition of these tools:

- have an appropriate understanding of the technology and algorithms used to provide digital advice (particularly they are able to understand the rationale, risks and rules behind the algorithms underpinning the digital advice); and

- are able to understand and review the digital/automated advice generated by the algorithms.

6. Guidelines on the format of the periodic statement for portfolio management of crypto-assets

6.1 Durable medium (Guideline 1)

Relevant legislation: Article 81(14) of MiCA.

106. Crypto-asset service providers should provide each such client with the periodic statement provided for in Article 81(14) of MiCA in a durable medium.

107. Such medium should enable a client to store the information addressed personally to that client in a way accessible for future reference and for a period of time adequate for the purposes of the information; and ii) allow the unchanged reproduction of the information stored.

6.2 Access to an online system (Guideline 2)

Relevant legislation: Article 81(14) of MiCA.

108. For the purposes of Article 81(14), subparagraph 2 of MiCA, crypto-asset service providers should ensure that:

- the online system their clients have access to qualifies as a durable medium;
- the client is notified electronically of where and how the information may be accessed (for instance, if the online system is a website, the client should be notified of the address of the website, and the place on the website where the information may be accessed);
- the client is notified when a new periodic statement is made available; and
- the information is accessible continuously through that online system and for such period of time as the client may reasonably need to inspect it.

6.3 Content of the periodic statement (Guideline 3)

Relevant legislation: Article 81(14) of MiCA.

109. To ensure that clients get a fair and balanced review of the activities undertaken, of the performance of the portfolio and of how the activities undertaken meet the preferences, objectives and updated information on the suitability assessment during the reporting period, the periodic statement should include, as a minimum:

- a statement of the contents and the valuation of the portfolio, including details of each crypto-asset held, its market value, or fair value if market value is unavailable and the cash balance, all at the beginning and at the end of the reporting period;

- the performance of the portfolio during the reporting period, including any tokens received for free for the continuity of operations of a proof-of-stake and proof-of-stake- blockchain consensus mechanisms (staking awards);

- the total amount of fees and charges incurred during the reporting period, itemising at least total management fees and total costs associated with execution, and including, where relevant, a statement that a more detailed breakdown will be provided on request;

- a comparison of performance during the period covered by the statement with the performance benchmark (if any) agreed between the crypto-asset service provider and the client;

- for each transaction executed during the period, the main characteristics of the relevant transaction.

110. Crypto-asset service providers should also specify the date of the last suitability assessment or its review and, if relevant, on which basis it was last updated (such as new information provided by the client causing a change in the client's profile, new criteria applied by the crypto-asset service provider…).

7.2.3 Draft guidelines on the procedures and policies, including the rights of clients, in the context of transfer services for crypto-assets

1 Scope

Who?

1. These guidelines apply to:

   a. competent authorities and

   b. crypto-asset service providers that act as providers of transfer services for crypto-assets on behalf of clients within the meaning of Article 3(1)(26) of MiCA.

What?

2. These guidelines apply in relation to Article 82 of MiCA.

When?

3. These guidelines apply as of [dd mm yyyy]

2 Legislative references, abbreviations and definitions

2.1 Legislative references

ESMA Regulation	Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC[35]
MiCA	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937[36]
TOFR	Regulation (EU) 2023/1113 of the European Parliament and the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849[37]

2.2 Abbreviations

EC	European Commission
ESFS	European System of Financial Supervision
ESMA	European Securities and Markets Authority
EU	European Union

[35] OJ L 331, 15.12.2010, p. 84.
[36] OJ L 150, 9.6.2023, p. 40–205.
[37] OJ L 150, 9.6.2023, p. 1–39.

3 Purpose

4. These guidelines, developed by ESMA in close cooperation with EBA, are based on Article 82(2) of MiCA. The objectives of these guidelines are to establish consistent, efficient and effective supervisory practices within the ESFS and to ensure the common, uniform and consistent application of the provisions in Article 82 of MiCA. In particular, they aim at providing more clarity on the requirements 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, in the context of transfer services for crypto-assets. In this regard, ESMA anticipates a corresponding strengthening of investor protection.

4 Compliance and reporting obligations

4.1 Status of the guidelines

5. In accordance with Article 16(3) of the ESMA Regulation, competent authorities and crypto-asset service providers shall make every effort to comply with these guidelines.

6. Competent authorities to which these guidelines apply should comply by incorporating them into their national legal and/or supervisory frameworks as appropriate, including where particular guidelines are directed primarily at financial market participants. In this case, competent authorities should ensure through their supervision that firms comply with the guidelines.

4.2 Reporting requirements

7. Within two months of the date of publication of the guidelines on ESMA's website in all EU official languages, competent authorities to which these guidelines apply must notify ESMA whether they (i) comply, (ii) do not comply but intend to comply, or (iii) do not comply and do not intend to comply with the guidelines.

8. In case of non-compliance, competent authorities must also notify ESMA within two months of the date of publication of the guidelines on ESMA's website in all EU official languages of their reasons for not complying with the guidelines.

9. A template for notification is available on ESMA's website. Once the template has been filled in, it shall be transmitted to ESMA.

10. Crypto-asset service providers are not required to report whether they comply with these guidelines.

5 Guidelines on the policies and procedures in the context of transfer services for crypto-assets

5.1 General provisions on the policies and procedures on transfer of crypto-assets (Guideline 1)

11. Crypto-asset service providers should establish, implement and maintain adequate policies and procedures (including appropriate tools) to ensure that, in good time before the client enters into any agreement for the provision of transfer services for crypto-assets, they provide the client, on a durable medium, with the information and conditions related to the transfer services for crypto-assets.

12. The information provided should include at least the following:

- the name of the crypto-asset service provider, the address of its head office, and any other address and means of communication, including electronic mail address, relevant for communication with the crypto-asset service provider;
- the name of the national competent authority in charge of supervising the crypto-asset service provider;
- a description of the main characteristics of the transfer service for crypto-assets to be provided;
- a description of the form of and procedure for initiating or consenting to a transfer of crypto-assets and withdrawing an instruction or consent, including the specification of the information that has to be provided by the client in order for a transfer of crypto-assets to be properly initiated or executed (including, how to authenticate);
- the conditions under which the crypto-asset service provider may reject an instruction to carry out a transfer of crypto-assets;
- a reference to the procedure or process established by the crypto-asset service provider to determine the time of receipt of an instruction or consent to a transfer of crypto-assets and any cut-off time established by the crypto-asset service provider;
- an explanation per crypto-asset, of which distributed ledger technology (DLT) network is supported for the transfer of this crypto-asset;
- the maximum execution time for the transfer of crypto-assets service to be provided;
- for each DLT network, the time or number of block confirmations needed for the transfer to be irreversible on the DLT network or considered sufficiently irreversible

in case of probabilistic settlement taking into account the rules and circumstances of the DLT network;

- all charges, fees or commissions payable by the client to the crypto-asset service provider in relation to the crypto-assets transfer service, including those connected to the manner in and frequency with which information is provided or made available and, where applicable, the breakdown of the amounts of such charges;

- the means of communication, including the technical requirements for the client's equipment and software, agreed between the parties for the transmission of information or notifications related to the crypto-asset transfer service;

- the manner in, and frequency with which, information related to the service of crypto-asset transfer is to be provided or made available;

- the language or languages in which the agreement referred to in Article 82(1) of MiCA will be concluded and communication during this contractual relationship undertaken;

- the secure procedure for notification of the client by the crypto-asset service provider in the event of suspected or actual fraud or security threats;

- the means and time period within which the client is to notify the crypto-asset service provider of any unauthorised or incorrectly initiated or executed transfers of crypto-assets as well as the crypto-asset service provider's liability, including maximum amount thereof, for unauthorised or incorrectly initiated or executed transfers;

- the right of the client to terminate the agreement on the provision of crypto-asset transfer services and the modalities to do so.

13. The policies and procedures relating to the transfer services of crypto-assets should ensure that the crypto-asset service provider provides the relevant information in easily understandable words and in a clear and comprehensible form.

14. The policies and procedures referred to in paragraph 11 should also ensure that:

- at any time during the contractual relationship related to the crypto-asset transfer services, the client should be able to access or receive, on request, the agreement referred to in Article 82(1) of MiCA as well as the information listed in paragraph 12, on a durable medium;

- the client is made aware, of any change to the information listed in paragraph 12 in good time before such change starts to apply.

15. Crypto-asset service providers should be able to provide the relevant information at the time of providing a copy of the draft agreement in Article 82(1) of MiCA.

5.2 Information on individual transfers for crypto-assets (Guideline 2)

16. Crypto-asset service providers should establish, implement and maintain adequate policies and procedures (including appropriate tools) to ensure that, after receipt of an instruction to transfer crypto-assets but before the execution of the transfer of crypto-assets, the crypto-asset service provider provides the client with at least the following information:

    - a brief and standardised warning as to whether and when the crypto-asset transfer will be irreversible or sufficiently irreversible in case of probabilistic settlement;
    - the amount of any charges for the crypto-asset transfer payable by the client and, where applicable, a breakdown of the amounts of such charges.

17. The adequate policies and procedures as referred to in the previous paragraph should also ensure that initiation or execution of the transfer does not take place before ensuring compliance with Article 14 of Regulation (EU) 2023/1113.

18. The policies and procedures referred to in the previous paragraph should also ensure that initiation or execution of the transfer does not take place before adequate steps have been taken to ensure compliance with Article 14 and other applicable provisions of TOFR, where applicable.

19. Crypto-asset service providers should establish, implement and maintain adequate policies and procedures (including appropriate tools) to ensure that, after execution of individual transfers for crypto-assets, the crypto-asset service provider provides the client with at least the following information:

    - the names of the originator and the beneficiary
    - the originator's distributed ledger address or crypto-asset account number;
    - the beneficiary's distributed ledger address or crypto-asset account number;
    - a reference enabling the client to identify each transfer of crypto-assets;
    - the amount and type of crypto-assets transferred or received;
    - the debit value date or the credit value date of the transfer of crypto-assets.
    - the amount of any charges, fees or commissions relating to the transfer of crypto-assets and, where applicable, a breakdown of the amounts of such charges.

20. The policies and procedures referred to in paragraph 16 should also cover the periodicity of the information listed in paragraph 16, any fees or charges incurred for the provision of the information and how the information is to be provided.

21. The information listed in paragraph 16 should be provided in a durable medium and, where not provided more frequently than once a month, free of charge.

22. Crypto-asset service providers should establish, implement and maintain adequate policies and procedures (including appropriate tools) to ensure, without prejudice to other applicable regulatory requirements, that, where a transfer of crypto-assets is rejected, returned or suspended, the client is provided with, at least, the following information:

- the reason for the rejection, return or suspension;
- if applicable, how to remedy the rejection, return or suspension;
- the amount of any charges or fees incurred by the client and whether reimbursement is possible.

5.3 Execution times and cut-off times (Guideline 3)

23. Crypto-asset service providers should establish, implement and maintain adequate policies and procedures relating to, at least:

- the cut-off times for instructions for the transfer of crypto-assets to be regarded as received on the same business day;
- the maximum execution times depending on the crypto-asset transferred;
- the number of block confirmations needed for the transfer of crypto-assets to be irreversible on the DLT, or sufficiently irreversible in case of probabilistic settlement, for each DLT network.

5.4 Rejection or suspension of an instruction to transfer crypto-assets or return of crypto-asset transferred (Guideline 4)

24. Crypto-asset service providers should establish, implement and maintain adequate risk-based policies and procedures for determining whether and how to execute, reject, return or suspend a transfer of crypto-assets. Such policies and procedures should particularly take into account the provisions of TOFR, as relevant and as specified in the European Banking Authority's Guidelines preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes.

5.5 Liability of the crypto-asset service provider (Guideline 5)

25. Crypto-asset service providers should establish, implement and maintain adequate policies and procedures determining the conditions of the liability of the crypto-asset service provider to clients in case of unauthorised or incorrectly initiated or executed transfers of crypto-assets.

7.2.4 Draft guidelines on the maintenance of systems and security access protocols in conformity with appropriate Union standards

Draft Guidelines

1 Scope

Who?

1. These guidelines apply to ‘offerors’ as defined in Article 3(1)(13) of Regulation (EU) 2023/1114 and persons seeking admission to trading of crypto-assets other than asset-referenced tokens or e-money tokens.

What?

2. These guidelines apply in relation to Article 14(1) of MiCA.

When?

3. These guidelines apply 60 calendar days from the date of their publication on ESMA’s website in all official EU languages.

2 Legislative references, abbreviations and definitions

2.1 Legislative references

ESMA Regulation	Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC[38]
MiCA	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) 1095/2010 and Directives 2013/36/EU and (EU0 2019/1937[39]

2.2 Abbreviations

EC	European Commission
ESFS	European System of Financial Supervision
ESMA	European Securities and Markets Authority
EU	European Union
ART	Asset-referenced token(s)
EMT	E-money token(s)

2.3 Definitions

Management body	means the body or bodies of an issuer, offeror or person seeking admission to trading, or of a crypto-asset service provider, which are appointed in accordance with national law, which are empowered to set the entity's strategy, objectives and overall direction, and which oversee and monitor management decision-making in the entity and include the persons who effectively direct the business of the entity as

[38] OJ L 331, 15.12.2010, p. 84.
[39] OJ L 150, 9.6.2023, p. 40.

	defined in Article 3, paragraph 1, point (27) of Regulation (EU) 2023/1114 of the European Parliament and of the Council.
ICT systems	means a system utilising technology for gathering, storing, retrieving, processing, analysing and transmitting information.[40]
ICT and security risk	means the risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs when the environment or business requirements change (i.e., agility). This includes security risks resulting from inadequate or failed internal processes or external events including cyber-attacks or inadequate physical security.
Access control	means controls to ensure that physical and logical access to ICT assets is authorised and restricted based on business and information security requirements.[41]
Offerors and persons seeking admission to trading	refers to the shortened form of 'offerors and persons seeking admission to trading other than asset-referenced tokens and e-money tokens', for the purposes of these guidelines.

3 Purpose

4. These guidelines are based on Article 14(1) of MiCA. The purpose of these guidelines is to specify the appropriate Union standards for offerors and persons seeking admission to trading as regards procedures and policies, including how they should maintain their systems (referred to throughout as ICT systems—see definition in 3.2.2) and security access protocols. These guidelines also aim to promote greater convergence in the interpretation and application of the MiCA provisions applicable to offerors and persons seeking admission to trading.

[40] See: ISO 30145:2020, Definition of 'Information and Communication Technology (ICT).
[41] See: ISO/IEC 27002:2022 on Information security techniques controls (link).

4 Status of the guidelines

5. In accordance with Article 16 of the ESMA Regulation, competent authorities should make every effort to supervise the implementation of these guidelines and offerors or persons seeking admission to trading should make every effort to comply with them.

6. Competent authorities with supervisory oversight of the entities in scope should incorporate these guidelines into their national legal and/or supervisory frameworks as appropriate, including where particular guidelines are directed primarily at crypto-asset market participants in their jurisdictions. In this case, competent authorities should use a risk-based approach in their supervision to ensure that firms comply with the guidelines.

5 Reporting requirements

7. Within two months of the date of publication of the guidelines on ESMA's website in all official EU languages, competent authorities with supervisory oversight of the entities in scope must notify ESMA whether they (i) comply, (ii) do not comply but intend to comply, or (iii) do not comply and do not intend to comply with the guidelines.

8. In case of non-compliance, competent authorities must also notify ESMA within two months of the date of publication of the guidelines on ESMA's website in all official EU languages of their reasons for not complying with the guidelines.

9. A template for notification is available on ESMA's website. Once the template has been filled in, it shall be transmitted to ESMA.

10. Offerors and persons seeking admission to trading are not required to report whether they comply with these guidelines.

6 Guidelines on the maintenance of systems and security access protocols in conformity with appropriate Union standards

6.1 General principle on proportionality (Guideline 1)

11. All offerors and persons seeking admission to trading are expected to make every effort to comply with the provisions set out in these guidelines in such a way that is proportionate to, and takes account of, the organisation's size, their internal organisation, and the nature, scope, complexity and riskiness of the services and products that they provide or intend to provide.

6.2 Administrative arrangements concerning systems and security access protocols (Guideline 2)

Administrative arrangements

12. The offeror or person seeking admission to trading should ensure an adequate internal governance and internal control framework in place for the maintenance of their ICT systems and mitigation of ICT and security risks. The offeror or person seeking admission to trading should also set clear roles and responsibilities for ICT functions, and ICT security risk management, including those for the management body and, if applicable, its committees

13. The offeror or person seeking admission to trading should ensure that the quantity and skills of the organisation's staff and budget resources are adequate to support ICT and security risk management processes, including those related to their ICT systems and access protocols, on an ongoing basis. Furthermore, the offeror or person seeking admission to trading should ensure that relevant staff members, including any key function holders, receive appropriate training on these ICT and security risks on an annual basis, or more frequently if necessary.

14. The management body of the offeror or person seeking admission to trading should have accountability for setting, approving and overseeing the implementation of the organisation's ICT and security risk management processes, including as it relates to their ICT systems and security access protocols.

Roles and responsibilities

15. The offeror or person seeking admission to trading should assign to staff within the organisation the responsibility for managing and overseeing ICT and security risks and ensure that monitoring of adherence to the ICT and security risk management arrangements is performed. It should ensure that ICT and security risks are identified, measured, assessed, monitored, and reported to the management body.

16. Offerors and persons seeking admission to trading should identify and manage their ICT and security risks by ensuring that the staff in charge of ICT systems, processes, and

security operations have appropriate processes and controls in place to monitor, identify, analyse, report, and manage such risks within the limits of the organisation's risk appetite.

17. The offeror or person seeking admission to trading should define and assign key roles and responsibilities to establish procedures and processes to:

- determine the risk appetite for ICT and security risks;
- identify and assess the ICT and security risks to which the organisation is exposed;
- define mitigation measures, including controls, to mitigate ICT and security risks;
- monitor the effectiveness of these measures and take action to correct the measures, where necessary;
- report to the management body on ICT and security risks and controls;
- identify and assess whether there are any ICT and security risks resulting from any major change in ICT system or ICT services, processes or procedures, and/or after any significant operational or security incident;
- manage cryptographic keys through their whole lifecycle.

6.3 Physical security access protocols (Guideline 3)

18. Offerors and persons seeking admission to trading should define, document, and implement physical security measures to protect their premises, data centres and sensitive areas from unauthorised access and from environmental hazards. The offeror or person seeking admission to trading should keep a record of each entry to those premises that require authorisation to access.

19. Physical access to ICT systems should be permitted to only authorised individuals according to the need-to-know, least privilege principles and on an ad-hoc basis. Authorisation should be assigned in accordance with the authorised individual's tasks and responsibilities and limited to individuals who are appropriately trained and monitored. Physical access should be reviewed annually to ensure that unnecessary access rights are promptly revoked when no longer required.

20. Adequate measures to protect from environmental hazards should be commensurate with the importance of the buildings and the criticality of the operations or ICT systems located in these buildings.

6.4 Security access protocols for ICT systems (Guideline 4)

21. Offerors and persons seeking admission to trading should ensure that logical access to ICT systems is restricted to authorised individuals designated by the offeror or person

seeking admission to trading. Authorisation should be assigned in accordance with the staff's tasks and responsibilities, and limited to individuals who are appropriately trained and monitored. Offerors and persons seeking admission to trading should institute controls that reliably restrict such access to ICT systems to those with a legitimate business requirement. Electronic access by applications to data and systems should be limited to the minimum that is required to provide the relevant service.

22. Offerors and persons seeking admission to trading should institute strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements. Controls such as role-based access, logging and reviewing of the ICT systems activities of privileged users, strong authentication, and monitoring for anomalies should be implemented. The offeror or person seeking admission to trading should manage access rights to information assets and their supporting systems on a need-to-know and least privilege basis. Access rights should be reviewed annually.

23. Access logs should be retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, without prejudice to the retention requirements set out in EU and national law. Offerors and persons seeking admission to trading should use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of their services.

24. Remote administrative access to critical ICT components should be granted only on a need-to-know and least privilege basis and only when strong authentication solutions are available.

25. The operation of products, tools and procedures related to access control processes should protect the access control processes from being compromised or circumvented. This includes enrolment, delivery, revocation and withdrawal of corresponding products, tools, and procedures.

6.5 Cryptographic key management (Guideline 5)

27. The offeror or person seeking admission to trading should be responsible for cryptographic key management as part of the roles and responsibilities assigned to key staff for ICT and security risk. These staff of the offeror or persons seeking admission to trading should be responsible for managing cryptographic keys through their whole lifecycle should include, generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking and destroying keys.

28. Offerors and persons seeking admission to trading should identify and implement controls to protect cryptographic keys through their whole lifecycle against loss, unauthorised access, disclosure and modification.

29. Offerors and persons seeking admission to trading should develop and implement methods to replace the cryptographic keys in the case of lost, compromised or damaged keys.

30. Offerors and persons seeking admission to trading should create and maintain a register for all certificates and certificate storing devices for at least critical ICT components. The register shall be kept up-to-date.

31. Offerors and persons seeking admission to trading should ensure the prompt renewal of certificates in advance of their expiration.