17 December 2024
ESMA75-223375936-6089

Final Report

Guidelines specifying Union standards on the maintenance of systems and security access protocols for offerors and persons seeking admission to trading of crypto-assets other than asset referenced tokens and e-money tokens

Table of Contents

List of acronyms

ART	Asset-referenced token
CASP	Crypto-asset service provider
CBA	Cost-benefit analysis
DLT	Distributed ledger technology
DORA	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA)
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
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
NIS2	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2).
RMF	Risk management framework
RTS	Regulatory technical standards

1 Executive Summary

Reasons for publication

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. MiCA empowers ESMA to develop technical standards and guidelines specifying certain provisions. ESMA is issuing these guidelines as mandated in Article 14(1), second subparagraph of MiCA.

On 25 March 2024, ESMA published a Consultation Paper to seek stakeholder feedback on ESMA's proposal for these guidelines under MiCA. The consultation period closed on 25 June 2024. Consultation responses (from stakeholders who consented to publication) are available on ESMA's website[2]. This Final Report explains how ESMA incorporated stakeholder feedback to prepare a final version of the guidelines.

ESMA also sought the advice of the Securities and Markets Stakeholder Group's (SMSG) established under Regulation (EU) No 1095/2010. The SMSG did not provide a response to the questions for consultation related to these guidelines.

Contents

Section 2 of the Final Report explains the legal basis for the guidelines and summarises ESMA's assessment of feedback provided to each of the consultation questions. These summaries provide a rationale for the changes between the draft guidelines provided in the consultation and those included in this Final Report. Major updates to the guidelines discussed in this section concerned the definitions, which have been overhauled to align more closely with the most relevant Union standards. The annexes to the Final Report are found in Section 3, which contains: (i) the cost-benefit analysis (Annex I), (ii) the summarised question-by-question feedback to the consultation (Annex II), and (iii) the final guidelines (Annex III).

Next Steps

The guidelines in Annex III of this final report will be translated into the official EU languages and published on the ESMA website. The publication of the translations will trigger a two-month period during which competent authorities must notify ESMA whether they comply or intend to comply with the guidelines. The guidelines will apply from three months after the publication of the translations.

[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).
[2] ESMA, Consultation on technical standards specifying certain requirements of MiCA – (3rd package). Link

2 Guidelines for the maintenance of systems and security access protocols in conformity with appropriate Union standards

2.1 Background and legal basis

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.*

1. Article 14(1) second subparagraph of MiCA mandates ESMA, in cooperation with EBA, to issue guidelines to specify the Union standards in conformity with which 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" under Article 14(1)(d) of MiCA.
2. 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 further requires offerors and persons seeking admission to trading of crypto-assets other than ART and EMT to (i) act honestly, fairly and professionally, (ii) communicate with prospective holders of the crypto asset in a fair, clear and not misleading manner, and (iii) identify, prevent, manage and disclose any conflicts of interest.
3. Further background on the mandate can be found in Recital 38, 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 understands '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. While the formulation of ‘security protocols’ in the recital is not identical to ‘security access protocols’ in the mandate, ESMA considers this difference insignificant.

2.2 Specification of the term ‘systems’ in the mandate

2.2.1 Proposal in the consultation

Question 14: Do you support ESMA’s interpretation of the term, ‘systems’ in the mandate?

4. 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. In the consultation paper, ESMA acknowledged that the term 'systems’ is ambiguous in this context. It may include concepts such as ‘business processes’, or it can be narrowly construed to only include certain types of systems that entities in scope could use in their activities. For the purposes of the draft guidelines, ESMA proposed using a narrow understanding: ‘ICT systems’. Stakeholders were asked whether they supported this interpretation.

5. The definition for ‘ICT system’ initially provided in the draft guidelines in the consultation was borrowed from the definition for ‘information and communications technology (ICT)’ in ISO 30145:2020: *a system utilising technology for gathering, storing, retrieving, processing, analysing and transmitting information*. Although the definition itself was not part of the question posed in the consultation, ESMA did not receive any comments about it. Nor did ESMA ask stakeholders in the consultation about the other definitions provided in the guidelines since these were not for interpretation and already exist in Union (or ISO) standards.

2.2.2 Feedback from stakeholders

6. Overall, ESMA received strong support from stakeholders for the narrow interpretation of systems (focused on ICT). Some respondents further suggested that the guidelines should explicitly list those ICT systems in scope and include cryptographic mechanisms, DLTs or blockchains, smart contracts, and private keys in this list.

7. Several respondents asked ESMA to clarify in the guidelines whether permissionless DLTs or decentralised protocols fall within or outside the scope of the ‘ICT systems’ concept. There was an even split between respondents who said decentralised systems should be in scope and those who said such systems should remain outside of scope. The argument respondents made for leaving them out of scope was the limited control offerors and people seeking admission to trading of crypto-assets would be able to exercise over decentralised systems.

8. Another respondent argued for the inclusion (in the understanding of ICT systems in the guidelines) of those systems that support governance and risk management procedures, such as KYC/AML software and trade monitoring systems.

2.2.3 ESMA's assessment and proposal

9. ESMA will maintain the narrow interpretation of 'systems' with a focus on ICT for the guidelines. Therefore, no changes have been proposed to the understanding of this definition. However, ESMA, on its own initiative, changed the definition provided for 'ICT systems' from the ISO definition to the more current precedent from the Network and Information Security Directive (EU) 2022/2555 (NIS2): 'network and information systems'. The rationale for this revision is to achieve closer alignment with other relevant Union standards.

10. In addition to updating the definition that serves as a more tangible stand-in for the more ambiguous term, 'systems', ESMA replaced references to 'ICT components' with the term 'ICT assets' to align with Article 3, point (7), of DORA (see this update in paragraphs 24 and 29 of the guidelines). The rationale for this replacement is the fact that 'ICT components' is not defined in any relevant Union standards. This alignment is also convenient considering the definition of 'ICT asset' is a subset of 'network and information systems' per the definition.

11. With respect to whether permissionless DLT and other types of decentralised protocols should be in scope of the term: 'network and information systems', ESMA considers the guidelines are sufficiently clear already: permissionless DLT and decentralised protocols are not considered a network and information system for the purposes of these guidelines because they would not be directly under the control of the offeror or person seeking admission to trading, nor would they be subject to contractual arrangements with a third-party provider. By extension, ESMA does not consider them as 'systems' per the terminology provided in the mandate. In addition, Guideline 1 emphasises the need for a proportional approach. Bringing permissionless DLT into the meaning of 'systems' in these guidelines would impose a burden on offerors or persons seeking admission to trading that would be disproportionate in light of their role in the crypto ecosystem (and raises questions about whether they would even be able to conform with the guidelines).

12. ESMA would expect offerors or persons seeking admission to trading to conform to the guidelines when the 'systems' in question are those that support compliance with other MiCA requirements (such as AML/CFT and trading surveillance software). When such systems are provided to the offeror or person seeking admission to trading by a third-party or via an intra-group outsourcing arrangement, as is often the case for compliance software, then ESMA would expect the offeror to ensure it has adequate administrative arrangements to mitigate any ICT risks that may emerge.

2.3 Precedent in other 'appropriate Union standards'

2.3.1 Proposal in the consultation

Question 15: Are there other 'appropriate Union standards' beyond those identified in the consultation paper that you consider relevant for this mandate?

13. In the consultation paper, ESMA explained that the draft guidelines are based primarily on the now published Commission Delegated Regulation (EU) 2024/1774 [3] which specifies standards on ICT and physical security access controls as part of the risk management measures for financial entities subject to DORA. ESMA used Article 21 of the Commission Delegated Regulation 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 addition, ESMA noted that 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), also served as a model (although ESMA considers some of the requirements in Article 16 inappropriate for offerors and persons seeking admission to trading considering the narrow MiCA mandate).

14. The consultation also cited EU Regulations or Directives, including pending technical standards or guidelines, that include measures for maintenance of systems and security access controls in the context of ICT security. Under NIS2, the Commission has prepared 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) [4] . Similarly, as part of Directive (EU) 2022/2557 (Critical Entities Regulation), the Commission's Critical Entities Resilience Group is also responsible for the preparation of guidelines on a range of resilience measures for so-called 'Critical Entities' which would include 'access controls[5]'.

15. Another precedent used in the development of these guidelines is the EBA Guidelines on ICT Information Security published in 2019[6]. Despite the banking sector focus (entities in scope include payment service providers and credit institutions) and the less current reference material, ESMA borrowed some of the 'evergreen' principles for administrative and governance arrangements from these guidelines.

16. Although there are other precedents in EU cybersecurity legislation that could meet the threshold of 'appropriate Union standards', many of the Union standards ESMA reviewed

[3] See: Article 21 of Commission Delegated Regulation (EU) 2024/1774 Commission Delegated Regulation (EU) 2024/1774 of 19 September 2024 Supplementing Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). 2024. EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1774.
[4] Commission Implementing Act pursuant to Art. 21(5) of Directive (EU) 2022/2555 (NIS2) (link)
[5] Guidelines pursuant to Art. 13(5) of Directive (EU) 2022/2557 (Critical Entities Regulation) (link). Note, these guidelines were not publicly available at time of publication of this Final Report.
[6] EBA/GL/2019/04 Final Report: EBA Guidelines on ICT and security risk management, 29 November 2019 (link)

for ICT security draw directly from ISO standards. In the consultation, ESMA explained that it also referred to the latest edition of relevant ISO standards (27002:2022) for confirmation to ensure the controls in the guidelines are based on the latest internationally-recognised best practices for operational resilience.

2.3.2 Feedback from stakeholders

17. In general, ESMA's proposal on the relevant Union standards to consider was deemed appropriate. Some respondents provided additional suggestions on other legal acts that could be relevant to the guidelines. In particular, respondents mentioned other EU measures related to operational resilience, namely NIS2 (which ESMA mentioned in the consultation), the Cyber Resilience Act and the TIBER-EU framework, as well as measures addressing data protection, including GDPR, and the eIDAS Regulation on trust services.

18. Outside of Union standards, one respondent noted the relevance of ISO 27001 and another suggested that ESMA consider the Payment Card Industry Data Security Standard (PCI DSS).

2.3.3 ESMA assessment and proposal

19. Many of these Union standards suggested by stakeholders are indeed relevant in terms of subject matter and were not considered prior to the consultation. However, ESMA finds that the additional suggestions provided in the feedback would not further contribute to the guidelines as not all of them are fit for purpose for the scope of the mandate. See ESMA's considerations below:

- The Cyber Resilience Act refers to consumer-focused hardware products. Among these are 'critical products with digital elements', including those using 'secure crypto-processing;
- The GDPR addresses personal client data, which is not relevant for these guidelines (offerors and persons seeking admission to trading would not collect client data in a systematic way matching the collection of personal client data by CASPs);
- The TIBER-EU framework would not meet the proportionality objectives, nor is a penetration testing regime envisioned in the mandate;
- eIDAS is not fit for purpose as it addresses entities that are considered 'trust service providers'.
- The Payment Card Industry Data Security Standard (PCI DSS) is not a Union standard and is primarily designed for payment card data. Other provisions already in MiCA would be more relevant in a crypto-asset context.

20. As noted above, the implementing measures mandated in NIS2 entered into application on 18 October 2024, and hence were not available before the publication of the draft guidelines in the consultation. The relevant sections of the annex of that regulation, which cover staff security training (8.2), cryptography (section 9) and access controls (section 11) are aimed at specific subset entities and do not depart significantly from the DORA precedents in the same subject areas[7]. As such, using these two precedents, ESMA, on its own initiative, modified the frequency of staff security training in paragraph 13 (in Guideline 2) and the review of access rights (in paragraphs 19 and 22 of Guidelines 3 and 4). Considering DORA and NIS2 measures do not designate a specific timeframe, ESMA no longer considers instituting annual frequencies as was initially in the pre-consultation draft of the guidelines proportionate to the entities in scope.

21. While preparing these guidelines, ESMA also encountered the provisions related to smart contracts in the Data Act[8], which entered into force in early 2024. Although it can be argued that smart contracts could constitute a 'system' for the purposes of the mandate, the Data Act provisions would be out of scope because they would only apply to *providers* of smart contracts. This framing would not be relevant for offerors and persons seeking admission to trading who would be *users* of smart contracts.

2.4 Administrative arrangements

2.4.1 Proposal in the consultation

Question 16: Do you agree with the inclusion of (minimal) administrative arrangements in Guideline 2?

22. In the consultation paper, ESMA emphasised the different legislative treatment of the entities in scope of MiCA. Unlike CASPs and issuers of ART or EMT, offerors and persons seeking admission to trading are not subject to DORA with its comprehensive set of obligations for ICT and security risk management, including governance arrangements. ESMA also noted that it considers the proportionality principle already embedded in the mandate itself, which acknowledges that the entities in scope do not pose the same market or investor protection risks as CASPs and issuers.

23. The approach in the draft guidelines presented for consultation reflects ESMA's understanding that the mandate is aimed at ensuring the entities in scope conform to a proportionate threshold of ICT and security requirements in absence of the more comprehensive DORA requirements. The draft Guideline 2 reflects this approach by ensuring that the entities in scope have in place 'light-touch' administrative arrangements

[7] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024. OJ L 269, 1–34. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402690
[8] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Strengthening the Security of Network and Information Systems within the Union (NIS2). 2023. EUR-Lex, https://eur-lex.europa.eu/eli/reg/2023/2854.

to oversee ICT and security risk management without demanding extensive measures such as business continuity plans or third-party risk management.

24. Although it is not explicitly mentioned in the mandate, Recital 38 of MiCA clarifies that offerors and persons seeking admission to trading should have 'effective administrative arrangements' to ensure their systems and security access protocols meet Union standards. The draft guideline thus lays out administrative arrangements that define how the function(s) in charge of ICT and security risk management should be staffed, trained, and resourced, and how it should report to the management body of the offeror or person seeking admission to trading.

2.4.2 Feedback from stakeholders

25. Three respondents said the guidelines should explicitly include a provision for a risk management framework and the associated control function to oversee it, while most of the remaining respondents agreed that the entities in scope should not be subjected to the same level of governance measures that would apply to CASPs or issuers of ARTs and EMTs. Those who support a more explicit provision for a control function to oversee the risk management framework said the guidelines should create a level playing field between CASPs / issuers and offerors and persons seeking admission to trading. Otherwise, there was support for allowing the entities in scope to assign roles to existing personnel within the organisation. One respondent also noted that Guideline 2 already lists many recognisable aspects of a standard risk management framework.

26. On the areas of overlap with DORA, one respondent suggested an additional guideline specific to managing third-party risks whereas another respondent called for more comprehensive measures for incident reporting. Lastly, one respondent called for a 'tiered' or 'proportional' approach to business continuity measures for entities in scope (note: the guidelines do not address business continuity measures).

2.4.3 ESMA's assessment and proposal

27. Most respondents supported the approach in the draft Guideline 2 as published in the consultation paper, therefore, ESMA has not proposed any changes in the Final Report.

28. Concerns from respondents about a level playing field between all entities in scope of MiCA are valid, but they should be addressed in light of the proportionality objectives embedded in the mandate. If the MiCA legislation intended to establish a completely level playing field, it would have subjected offerors and persons seeking admission to trading to the same measures for CASPs and issuers.

29. As for the suggestions to incorporate other aspects of DORA governance arrangements into these guidelines, ESMA considers this out of scope of the mandate. The mandate is strictly focused on 'maintenance of their systems and security access protocols', which leaves no space for additional policy considerations for third-party risk management or incident reporting.

30. On its own initiative, ESMA added to the provisions in Guideline 2 (points ii, iii, and vi. of paragraph 17) for offerors to have in place adequate arrangements to also identify and mitigate ICT risks that may originate from third-party providers of ICT services that would constitute a 'system'. Point (ii) has also been extended to explicitly include the identification of risks associated with third-party dependencies. Although this was not a question in the consultation, the uncertainty as to whether the term 'systems' would include those provided by third-parties or through other intra-group outsourcing arrangements did emerge in the feedback. These additions in paragraph 17 serve to clarify that the offeror's ICT risk management arrangements should also cover risks related to systems that are provided through third-party ICT service providers.

31. Also on its own initiative, ESMA removed the provisions in the guidelines that implied entities in scope should manage risks 'within the limits of the organisation's risk appetite'. The concept of a 'risk appetite' or risk tolerance levels is not relevant for these guidelines because the sophistication of the network and information systems maintained by entities in scope is not expected to be varied enough to justify such a concept. Put another way: the level of 'acceptable' risk should never fall below a baseline that would ensure continuity and good functioning of their systems.

2.5 Cryptographic key management

2.5.1 Proposal in the consultation

Question 17: Do you support the inclusion of Guideline 5 on 'cryptographic key management'?

32. In the draft Guideline 5 published in the consultation paper, ESMA followed the precedent set in Article 7 on 'cryptographic key management' found in Commission Delegated Regulation (EU) 2024/1774 (the DORA Risk Management Framework or 'RMF').[9] However, the draft guideline departs from DORA by not including a provision for offerors and persons seeking admission to trading to establish a specific policy on cryptographic key management. Instead, the guideline provides for those entities in scope to have designated adequate staff for managing the specific ICT risks associated with the use of cryptographic keys. Hence, this is why ESMA included 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. Rather than a specific 'policy', ESMA has elected to include cryptographic key management in the regular ICT management arrangements of the offeror or persons seeking admission to trading.

33. Considering the importance of cryptographic key management in the activities of offerors and persons seeking admission to trading, ESMA believes that tailoring the requirements in the DORA RMF (those applicable to CASPs and issuers) for the same type of network and information systems would meet the standard of 'conformity with appropriate Union

[9] See: Article 7 of Commission Delegated Regulation (EU) 2024/1774

standards'. It would also create a level playing field among all the entities in scope of MiCA with some adjustment for proportionality. Although offerors and persons seeking admission to trading will not be custodians of client crypto-assets, they will custody their own crypto-assets (e.g., before transferring them to participants of an offer or depositing them on a trading platform for crypto-assets). So, the compromise of the private keys of the offeror or person seeking admission to trading could have wider repercussions for the value of any affected crypto-assets. That said, these risks are less acute than a key compromise in the context of service provision in which clients could suffer a complete loss of their crypto-assets.

2.5.2 Feedback from stakeholders

34. One respondent noted the omission of a provision in the draft guideline for offerors and persons seeking admission to trading to establish a specific policy on cryptographic key management and suggested that ESMA include such a requirement. In particular, this respondent said the policy should also be disclosed to clients when providing custody services (or even when the offeror or person seeking admission to trading holds crypto-assets in their own reserve or account).

35. A respondent objected to ESMA's implication in the consultation paper that cryptographic keys can be 'replaced'. Instead, this respondent said, the provision should require offerors or persons seeking admission to trading to prevent fraudulent transfers when keys are compromised and assume costs (from clients) of migration of crypto-assets to newly generated keys. Another respondent requested that ESMA clarifies that if a holder loses their private keys, they cannot be replaced if backups are not maintained, adding that it is standard risk management practice in the industry for some environments to perform regular key renewals to prevent keys from being used beyond a secure lifespan.

36. One respondent representing an industry-backed standard-setting group shared a set of industry-developed guidelines for risk management specific to cryptographic keys.[10] Another respondent asked for a provision in the guidelines that would ensure offerors or persons seeking admission to trading consider using multi-party computation (MPC) wallets (in which access to the crypto-assets is controlled by multiple private keys) as a 'best practice' for safekeeping of crypto-assets by avoiding a single point of compromise.

37. Two respondents suggested that ESMA should specify what is meant by 'cryptographic key management'. They asked ESMA to clarify the precise 'systems' understood within this technical concept, such as 1) authentication keys used in scenarios related to traditional ICT (e.g. encryption of communication channels, encryption of data at-rest, etc.), and 2) for private cryptographic keys used specifically in the context of crypto-assets and blockchains in general (e.g. to authorise and sign transactions on a blockchain, prove ownership of crypto-assets, etc.).

[10] See: CryptoCurrency Certification Consortium (C4). "CCSS Details." *CryptoCurrency Certification Consortium (C4)*, https://cryptoconsortium.org/cryptocurrency-security-standard-documentation/details/.

2.5.3 ESMA's assessment and proposal

38. Based on consultation feedback, ESMA does not intend to make any changes to the draft Guideline 5. The guideline as published in the consultation is aligned with the next closest set of standards for cryptographic keys in DORA.

39. Despite the suggestion from stakeholders, ESMA elected not to include a provision in the draft guideline for a specific policy on cryptographic key management for the reasons described in the consultation. While offerors and persons seeking admission to trading would be responsible for managing risks related to systems for cryptographic keys in line with the DORA standards, requiring a written policy runs counter to the proportionality objectives in the guidelines when these entities would not necessarily be providing client-facing services. Furthermore, as entities in scope of the guidelines would not be providing custody services (and if they do so they would need to be authorised as CASPs and hence subject to DORA), no client-facing disclosures of such a type of policy (as suggested by one respondent) would be necessary.

40. ESMA appreciates the suggestion that offerors and persons seeking admission to trading assume costs of migrating crypto-assets to newly generated keys in the scenario of a compromise. However, as the entities in scope would not be engaged in provision of crypto-asset services, they would always assume the costs for migration to new keys. In other words, such costs could not be passed on to clients as predicted by one respondent. Further, the guidelines already envision regular back-up and renewal of keys in line with industry standards.

41. As for the term 'replace' in paragraph 29 (Guideline 5), ESMA notes that this term is borrowed directly from DORA. Here it implies 'migrated' as 'replacing' private crypto keys may not be technically feasible depending on our understanding of the term.

42. While a direct reference to MPC wallets in the guidelines is an understandable suggestion from respondents, ESMA has not included such a reference in the guideline for two reasons: 1) CASPs and issuers would not be subjected to the same provisions under their relevant risk management measures in MiCA and DORA, and 2) MPC wallets do not appear in any pre-existing Union standards. Given the pace of technological progress in the area of cryptography, ESMA has elected to maintain a principles-based approach in these guidelines. In other words, the industry is best-suited to determine best practices for securing cryptographic keys and adapting to new technological solutions when they emerge.

43. ESMA clarifies that the term 'cryptographic key management' is meant to encompass any systems that make use of encryption, meaning it should be understood to include authentication keys in the traditional ICT sense as well as the blockchain-specific application of cryptography, both of which are relevant for the entities in scope of the guidelines. As the guidelines are principles-based, a distinction between these different applications of encryption technology is not strictly necessary for entities in scope to conform with the provisions.

3 Annexes

3.1 Annex I: Cost-benefit analysis

Impact of the guidelines in relation to Article 14(1)(d) of MiCA

1. According to Article 16(2) of Regulation (EU) No 1095/2010, any guidelines developed by ESMA shall be accompanied by an analysis of “the potential costs and benefits”.

2. This section presents the cost-benefit analysis (CBA) of the main policy options included in this final report for the requirements in the guidelines on the maintenance of systems and security access protocols.

Problem identification

3. A subset of entities under MiCA—offerors and persons seeking admission to trading of crypto-assets other than ARTs and EMTs —are not subject to DORA provisions for ICT risk management. MiCA appears to acknowledge that the relevant DORA provisions would be too burdensome for these entities, whose size, scale, and complexity do not rival that of CASPs or issuers of ARTs or EMTs. As an alternative, the mandate in MiCA requires those entities to manage their systems, including access protocols, in conformity with Union standards, leaving the details on how they should conform to those standards to be specified by ESMA through guidelines.

Policy objectives

4. The objective of these guidelines is to give guidance to offerors and persons seeking admission to trading to have effective administrative arrangements in place to mitigate circumstances that would threaten the integrity of their ICT and physical systems. This objective is framed within the wider goal of proportionality, meaning the measures in the guidelines should be commensurate with the size and scale of the entities in scope.

Baseline scenario

5. In the baseline scenario, offerors and persons seeking admission to trading would be subject to the requirements of Article 14(1) point (d) without any indication of which Union standards would be considered appropriate and how to adequately conform to those standards. The result would be a disparity in the levels of rigour applied by entities in scope to compliance with the mandate. This uneven application could have (hypothetical) repercussions in the market in the event of a compromise of an offeror’s systems.

6. It should also be noted that almost all of the costs for offerors and persons seeking admission to trading (and hence the benefits) relate to obligations in the MiCA basic act—not these guidelines. ESMA has indicated where this distinction is relevant throughout the CBA.

Options considered and preferred options

Policy issue 1: Staff training on ICT and security risks (paragraph 13, Guideline 2)

7. ESMA considered three policy options:

Option 1a: Provide for annual training for the staff with responsibility for ICT and security risk management within the organisation.

Option 1b: Provide for staff training but allow the entities in scope to determine the acceptable frequency of those trainings.

Option 1c: Do not require training for staff with responsibility for ICT and security risk management to train staff.

8. ESMA selected option 1b.

Costs

9. The costs associated with this policy choice would only be borne by offerors or persons seeking admission to trading. Annual training as in option 1a creates a recurring operational cost for the entities in scope, including time and resources spent on preparing, delivering, and receiving that training (if done in-house), or in fees paid to external experts or a third-party training provider. Entities may also provide role-specific training (for key function holders or high-level staff with responsibility for key management) may require highly specialised external trainers or certification programs, which can be more expensive than general training. In any case, in order to contain the burden for the relevant entities and ensure that the training is adapted to their risks and needs, the guidelines refer to periodic training.

10. Entities may also incur compliance costs around monitoring the organisation's adherence to the training requirement. For example, offerors or persons seeking admission to trading may require new systems to track who has completed the training and update the curriculum in response to evolving threats or regulatory changes. Maintaining records of these activities and demonstrating compliance during regulatory audits adds to administrative overhead.

Benefits

11. Allowing entities in scope to choose the frequency of their staff training as in option 1b provides more flexibility and aligns with DORA precedents. From a proportionality

perspective, these smaller entities may not have high turnover or hiring rates for staff in the ICT risk management part of the business that would require an *annual* cadence of trainings.

12. More generally, a provision on staff training should facilitate proper implementation of access controls, identifying vulnerabilities in network and information systems, and management cryptographic keys. As staff become more knowledgeable and skilled, offerors and persons seeking admission to trading may experience fewer operational disruptions and a reduction in the time spent addressing ICT-related issues, ultimately improving operational efficiency. In this scenario, rejecting option 1c can be considered a net benefit even if it means the entities in scope could avoid some of the ongoing costs associated with compliance.

Policy issue 2: Administrative arrangements, including the proportionality of the risk management provisions (paragraph 17, Guideline 2)

13. ESMA considered two policy options:

Option 2a: Subject offerors and persons seeking admission to trading to the simplified risk management framework (RMF) under DORA Article 16 and associated Commission Delegated Regulation specifying it further[11].

Option 2b: Take a bespoke approach in the guidelines for the entities in scope, based on 'evergreen' principles borrowed from other entity-specific guidelines prepared by the ESAs.

14. ESMA has selected option 2b. Given the narrow room for manoeuvre provided to ESMA in listing the administrative arrangements of the offeror or person seeking admission to trading per Recital 38, it is difficult for ESMA to justify a more intensive set of provisions based on the DORA simplified RMF, which requires business continuity plans and intensive oversight of third-party dependencies.

Costs

15. No additional costs associated with the specific risk management provisions in paragraph 17. It is understood that the offeror or person seeking admission to trading would simply have to 'assign roles and responsibilities' instead of creating a new risk control function for the purposes of the guidelines.

Benefits

16. By having the option to designate existing staff and/or resources to ensure the offeror's conformity with the provisions in the guidelines, entities in scope would avoid the

[11] OJ L, 2024/1774, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1774/oj

operational costs associated with the more burdensome approach in the DORA simplified RMF.

Table: Costs and benefits associated with the guidelines on systems and security access protocols

Stakeholder groups affected	Costs	Benefits
Offerors and persons seeking admission to trading	As it relates directly to the guidelines, the only costs would come from the requirement for annual or more frequent training for relevant staff on ICT and security risk management. Otherwise, offerors and persons seeking admission to trading will need to ensure that they have sufficient staff with the necessary skills to maintain network and information systems and mitigate security risks, including managing cryptographic keys. Recruitment and staffing to conform with these provisions would also incur operational costs for the entities in scope. But these costs originate from level 1 of MiCA, not from the guidelines.	By adhering to these guidelines, entities in scope will benefit from improved ICT security and resilience. A clear governance structure and assignments of responsibility for managing ICT risks help ensure that systems are protected against internal and external threats. Effective security access protocols and cryptographic key management reduce the risk of data breaches and other cybersecurity incidents, with their associated reputation and financial costs.
Competent authorities	Ongoing costs to supervise conformity with the guidelines. (*These costs originate from level 1*)	Supervisors will know that offerors and persons seeking admission to trading have implemented baseline ICT and security risk management protocols.
Other stakeholders (e.g., investors)	No direct costs for investors or other stakeholders.	Secondary effects of a data breach or compromise of crypto-assets held by the offeror or persons seeking admission to trading.

3.2 Annex II: Question-by-question responses

Question 14

1. Most respondents supported ESMA's interpretation of 'systems'. Some respondents further suggested that the guidelines explicitly list the systems in scope and include cryptographic mechanisms, DLTs or blockchains, smart contracts, and private keys. Several respondents also called for clarity on the definition of 'system' in the draft guidelines as it relates to permissionless DLTs.

2. Several respondents offered a list of ICT systems, encompassing the hardware, software, networks, databases, and technologies that support the operations, data processing, and communication functions of the entities in scope. Data encryption systems was also listed by one respondent.

3. One respondent said the guidelines should account for 'distant service providers' to comply with the requirements.

4. Several respondents remarked on the use of the term 'business processes' in the draft guidelines, which was considered more ambiguous than 'ICT systems'—the preferred term because it is 'measurable' and can be 'standardised'.

5. One respondent argued for the explicit inclusion in the guidelines of systems in support of governance and risk management procedures, such as KYC/AML software and trade monitoring systems.

Question 15

6. Respondents suggested ESMA review other relevant EU legislation or international standards, including the following:

   - Network and Information Systems Directive (NIS2) and the Cyber Resilience Act;
   - TIBER-EU framework;
   - GDPR;
   - eIDAS Regulation;
   - ISO 27001 on Information Security Management.

7. One respondent suggested that ESMA consider the aspects of the NIS2 Directive relevant for 'operators of essential services' which may be relevant for crypto entities. The same respondent also cited the Payment Card Industry Data Security Standard (PCI DSS) for sensitive financial information as a relevant standard in the context of the guidelines.

8. Respondents called for general alignment with EU legislation on data protection and IOSCO standards.

9. One respondent asked ESMA to consider all the ICT security areas that are included in DORA for CASPs and issuers of ARTs and EMTs.

Question 16

10. Three respondents said the guidelines should explicitly include a provision for a risk management framework and the associated control function to oversee it, citing a level playing field between the entities in scope of MiCA.

11. Most of the remaining respondents agreed that the entities in scope should not be subjected to the same level of governance measures that would apply to CASPs or issuers of ARTs and EMTs. There was also support for allowing the entities in scope to assign roles to existing personnel within the organisation.

12. One respondent also noted that draft Guideline 2 already lists many recognisable aspects of a standard risk management framework.

13. One respondent suggested an additional guideline specific to managing third-party risks whereas another respondent called for more comprehensive measures for incident reporting. Lastly, one respondent called for a 'tiered' or 'proportional' approach to business continuity measures for entities in scope (*note: the guidelines do not address business continuity measures as it is not in the mandate*).

Question 17

14. One respondent suggested a requirement that offerors and persons seeking admission to trading prepare (and publish) a specific policy on encryption and cryptographic controls that clients can easily view or access at any time. Such a policy would be required for providing custody services or when the offeror or person seeking admission to trading holds crypto-assets within their reserve of assets.

15. One respondent suggested a reformulation of one of the provisions in draft guideline no. 5 in the consultation paper so as not to imply that cryptographic keys can be 'replaced'. Instead, the provision should require offerors or persons seeking admission to trading to prevent fraudulent transfers when keys are compromised and assume costs of migration of crypto-assets to newly generated keys, this respondent said.

16. One respondent representing an industry-backed standard-setting group shared a set of industry-developed guidelines for risk management specific to cryptographic keys.[12]

[12] See: CryptoCurrency Certification Consortium (C4). "CCSS Details." *CryptoCurrency Certification Consortium (C4)*, https://cryptoconsortium.org/cryptocurrency-security-standard-documentation/details/.

17. Two respondents suggested specifying that ‘cryptographic key management’ should exist for both: 1) authentication keys used in scenarios related to traditional ICT (e.g. encryption of communication channels, encryption of data at-rest, etc.), and 2) for private cryptographic keys used specifically in the context of crypto-assets and blockchains in general (e.g. to authorise and sign transactions on a blockchain, prove ownership of crypto-assets, etc.).

18. One respondent requested that ESMA clarify that if a holder loses their private keys, they cannot be replaced if backups are not maintained. This same respondent said that from a maintenance perspective, it is standard practice for some environments to perform regular key renewals to prevent keys from being used beyond a secure lifespan.

19. One respondent asked for a provision in the guidelines that would ensure offerors or persons seeking admission to trading consider using multi-party computation (MPC) wallets (in which access to the crypto-assets is controlled by multiple private keys) as a sort of ‘best practice’ for safekeeping of crypto-assets and to avoid a single point of compromise.

3.3 Annex III: Guidelines

Guidelines specifying Union standards on the maintenance of systems and security access protocols for offerors and persons seeking admission to trading of crypto-assets other than asset referenced tokens and e-money tokens

3.3.1 Scope

Who?

1. These guidelines apply to competent authorities and to 'offerors' as defined in Article 3(1)(13) of MiCA 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), point (d), 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.

3.3.2 Legislative references, abbreviations and definitions

1.1. 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.[13]
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.[14]
NIS2 Directive	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.[15]
DORA	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.[16]

1.2. Abbreviations

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

1.3. Definitions

[13] OJ L 331, 15.12.2010, p. 84.
[14] OJ L 150, 9.6.2023, p. 40.
[15] OJ L 333, 12.12.2022, p. 80–133.
[16] OJ L 333, 14.12.2022, p. 1–79.

network and information system	means 'network and information system' as defined in Article 6, point (1) of NIS2 Directive.
ICT risk	means 'ICT risk' as defined in Article 3, point (5), of DORA.
ICT asset	means 'ICT asset' as defined in Article 3, point (7), of DORA.
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.[17]
offerors and persons seeking admission to trading	refers to the shortened form of 'offerors and persons seeking admission to trading of crypto-assets other than asset-referenced tokens and e-money tokens', for the purposes of these guidelines.

3.3.3 Purpose

4. These guidelines, prepared in cooperation with the European Banking Authority, are based on Article 14(1), point (d), of MiCA. The purpose of these guidelines is to specify the appropriate Union standards for offerors and persons seeking admission to trading as regards the maintenance of systems and security access protocols, including policies and procedures. 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.

[17] *ISO/IEC 29146:2016 Information technology — Security techniques — A framework for access management*. International Organization for Standardization, 2016.

3.3.4 Status of the guidelines

5. In accordance with Article 16 of the ESMA Regulation, competent authorities must 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 to which these guidelines apply 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 ensure through their supervision that financial market participants comply with the guidelines.

3.3.5 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 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 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.

3.3.6 Guideline 1: General principle on proportionality

11. Offerors and persons seeking admission to trading are expected to make every effort to comply with these guidelines in such a way that is proportionate to, and takes account of, the organisation's size, its overall risk profile, and the nature, scope, and complexity of its activities or operations.

3.3.7 Guideline 2: Administrative arrangements concerning systems and security access protocols

Administrative arrangements

12. The offeror or person seeking admission to trading should ensure an adequate internal governance and internal control framework is in place for the maintenance of their network and information systems and mitigation of ICT risks. The offeror or person seeking admission to trading should also set clear roles and responsibilities for functions with responsibility for ICT risk management.

13. The offeror or person seeking admission to trading should ensure that the skills of their staff and their budget resources are adequate to support ICT risk management arrangements, with particular reference to those staff responsible for maintenance of network and information systems and access controls, on an ongoing basis. Furthermore, the offeror or person seeking admission to trading should ensure that relevant staff members, including any key function holders, periodically receive appropriate training on ICT risks.

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 risk management arrangements, including as it relates to their network and information systems and access controls.

Roles and responsibilities

15. The offeror or person seeking admission to trading should assign to staff within the organisation the responsibility for appropriately identifying, managing, and overseeing ICT risks. It should ensure that the staff in charge of managing ICT risk and security operations have appropriate arrangements in place to identify, monitor, assess, and report on those ICT risks.

16. The offeror or person seeking admission to trading should ensure that the staff responsible for managing the ICT risks associated with network and information systems and access controls is able to ensure that the identified ICT risks are monitored, assessed, and reported to the management body.

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

    i. identify and assess the ICT risks, including those related to ICT services provided by third-party service providers, to which the organisation is exposed;

    ii. define mitigation measures, including controls to mitigate ICT third party risks;

    iii. monitor the effectiveness of the measures referred to in point ii. and take action to correct the measures, where necessary;

    iv. report to the management body on ICT risks and mitigation measures;

    v. identify and assess whether there are any ICT risks resulting from any major change in network and information systems or ICT services (including where provided by third parties), or after any significant operational or security incident;

    vi. manage cryptographic keys through their whole lifecycle.

3.3.8 Guideline 3: Physical security access protocols

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 network and information 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 periodically reviewed and withdrawn 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 network and information systems located in these buildings.

3.3.9 Guideline 4: Security access protocols for network and information systems

21. Logical access to network and information systems should be 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 whose access to the systems is monitored. Offerors and persons seeking admission to trading

should institute controls that reliably restrict such access to network and information 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 network and information 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. Logical access rights should be periodically reviewed and withdrawn when no longer required.

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 assets 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 those access control processes from being compromised or circumvented. This includes enrolment, delivery, revocation and withdrawal of corresponding products, tools, and procedures.

3.3.10 Guideline 5: Cryptographic key management

26. 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 risk. These staff of the offeror or persons seeking admission to trading should be responsible for managing cryptographic keys through their whole lifecycle, including, generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking and destroying keys.

27. 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.

28. 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.

29. 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 assets. The register should be kept up-to-date.

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