LEXIFY INSIGHTS

YOUR TRUSTED LEGAL NEWSLETTER

ESMA ON THE CRYPTO ASSET SERVICE PROVIDER AUTHORIZATION

Digital Assets | 01/2025

Introduction

On January 31, 2025, the European Securities and Markets Authority ("**ESMA**") issued a supervisory briefing containing guidance (hereinafter, the "**Guidance**") on the authorization of Crypto Asset Service Providers ("**CASPs**") under Title V of Regulation (EU) 2023/1114 (hereinafter, "**MiCAR**").

Before delving into the details of the Guidance, we would like to highlight ESMA's unequivocal stance regarding CASPs. Specifically, ESMA states that: "*There are no low-risk CASPs* […] *There should therefore be no instances where a cursory assessment, based on a 'low-risk' categorization, could exist*."

This statement underscores ESMA's position that no CASP should be presumed low-risk, emphasizing the necessity for thorough and comprehensive assessments in all cases.

ESMA Guidance Key Findings

ESMA's Guidance focuses on the following key aspects:

- risk factors that increase regulatory concerns for CASPs;
- substance and governance requirements for CASPs, including but not limited to minimum standards, insufficient local autonomy, and outsourcing of functions to non-EU jurisdictions;
- outsourcing of critical functions;
- so-called "*Fit and Proper*" assessment of key personnel; and
- other authorization-related requirements.

Elements Constituting Elevated Risk

In the context of the authorization process under Article 59 of MiCAR, National Competent Authorities ("**NCAs**") are advised to apply an elevated level of scrutiny based on several key risk factors, including but not limited to:

- **size**: larger CASPs - defined as **those exceeding 1,000,000 active yearly users or maintaining a balance sheet size above €3 billion**[1]—pose a heightened risk potential in the event of non-compliance. However, this does not imply that CASPs operating below

[1] Section 3.2 of the Guidance.

these thresholds are exempt from rigorous scrutiny by NCAs;

- **cross-border operations**: CASPs with significant user bases outside their home Member State necessitate enhanced coordination among NCAs to ensure compliance with MiCAR's regulatory framework across jurisdictions;
- **combination of CASP and issuer functions**: CASPs that engage in both issuer and service provider activities (e.g., issuance of Asset-Referenced Tokens ("**ARTs**") or E-Money Tokens ("**EMTs**") alongside CASP functions) are subject to intensified scrutiny due to potential conflicts of interest, as further detailed in the relevant second-level European regulations[2]; and
- **outsourcing of key functions**: particular caution is required when core operational functions - such as compliance, risk management, or ICT security - are outsourced either within the same group or to third countries.

Substance and Governance of CASPs

ESMA explicitly stipulates in its Guidance that at least one member of the executive management board **must be located in the relevant EU jurisdiction**. However, exceptions may apply for Member States with populations below one million (e.g., Malta, Luxembourg), provided that board members are available on short notice (not exceeding two business days) for in-person meetings with regulatory authorities.

All CASPs outsourcing essential functions to non-EU jurisdictions will be subject to heightened scrutiny. While outsourcing of support functions, such as IT and HR, is generally permissible, one indicator of regulatory concern is the proportion of costs allocated outside the EU. Accordingly, CASPs with limited managerial and operational presence in the EU and those operating within large corporate groups outside the European regulatory framework should undergo detailed legal assessments.

ESMA has further established parameters to evaluate the autonomy of CASPs, focusing on:

- the CEO's exclusive dedication to CASP-related activities, while allowing for greater flexibility for other management members;
- executive management board members' deep familiarity with both national and EU regulatory frameworks;
- the requirement **for at least one executive management board member to reside in the EU** Member State where the authorization is granted. In cases involving Member States with populations under one million, board members

[2] ESMA, *Final Report Draft technical Standards specifying certain requirements in relation to conflicts of interest for crypto-asset service providers under the Markets in Crypto Assets Regulation (MiCA)*, ESMA18-72330276-1634, 31 May 2024.

may be based in a directly neighboring country, provided they are available for in-person engagements within two business days; and

- the authorized EU entity's capacity to exercise sufficient decision-making power, independent of non-EU affiliates.

Regarding internal control functions, CASPs are advised to maintain clear delineations of responsibilities. For smaller CASPs, risk management and compliance functions may be combined, provided that they remain separate from each other and that clear reporting lines to the management body are established, like for example outlined in standard Internal Procedures Manuals of many EU investment firms. Additionally, best practices suggest that CASPs should define their specific risk approach through comprehensive risk matrices, scenario analyses, and stress testing across financial, ICT, AML, and legal domains.

In line with financial intermediary regulations, ESMA emphasizes that CASPs must maintain a compliance plan subject to annual reviews and updates in the event of material changes.

Finally, ESMA reminds NCAs to carefully assess cases where parts of a CASP's staff are outsourced outside the EU jurisdiction where authorization was granted. In this regard, it is noteworthy that regulatory authorities must ensure that such outsourcing arrangements do not compromise effective oversight, including information access and operational continuity.

Outsourcing of CASPs critical functions

ESMA stressed that core functions may not be outsourced to the extent that the CASP effectively becomes a so-called "*letter-box entity*."[3]

Particular attention must be given to compliance with the Regulation (EU) 2022/2554 Digital Operational Resilience Act ("**DORA**"), applicable as of January 17, 2025, regarding ICT service outsourcing and related contractual requirements. A key provision reaffirmed in ESMA's Guidance is that responsibility for compliance, particularly in the AML and ICT domain, **cannot be delegated to third-party providers**. CASPs remain ultimately accountable for ensuring regulatory adherence (See section 5.1 of the Guidance[4]) to MiCAR and DORA.

What can be inferred from the Guidance is that the primary concern for ESMA appears to be the outsourcing and sub-outsourcing of services to providers lacking the necessary resources or time to deliver adequate services. To mitigate these risks, CASPs are encouraged to implement robust Service Level Agreements ("**SLAs**") to gain full visibility into any sub-outsourcing arrangements.

[3] Section 5.1. of the Guidance.

[4] See also Art. 73(1)(a) of MiCAR and Art. 5(2)(a) of DORA with respect to cybersecurity risks.

Fit and Proper Assessment of Key Individuals

In its Guidance, ESMA provides detailed provisions on the assessment of individuals who hold control over CASPs. Specifically, NCAs must consider whether **prior EU or non-EU supervisory infractions** could elevate an authorization to a higher risk category.

As per the skills and the experience of management and/or CASPs key-personnel, ESMA places greater emphasis on technical expertise in the crypto sector over general managerial experience. However, a lack of management experience may, in principle, be offset by the presence of executive board members with robust backgrounds in regulated financial industries.

Finally, NCAs must assess whether ongoing criminal proceedings involve an entity, its management body members, shareholders, or individuals holding qualifying interests, even in the absence of a final conviction. This includes cases of guilty pleas and pending judicial investigations within and outside the EU.

Conclusion

ESMA's Guidance underscores its commitment to ensuring that the regulatory framework for CASPs under MiCAR remains robust and comprehensive. NCAs are expected to implement rigorous oversight and enforcement measures to mitigate risks associated with CASP operations, thereby fostering market integrity and investor protection in the evolving crypto-asset landscape.

For businesses seeking assistance in navigating the complexities of MiCAR authorization, particularly non-EU entities looking to establish a presence within the European regulatory framework, Lexify provides the right legal support.

Contact us to safeguard your crypto business's future in the EU market.

Contact

Connect with us

Thank you for taking the time to read our article. We hope you find it informative and engaging. If you have any questions, feedback, or would like to explore our services further, we're here to assist you.

Emanuele Gambula

+41 76 232 66 83

emanuele.gambula@lexify.io

Contact Information

For inquiries about our legal assistance, please contact:

- **Email:** Emanuele.gambula@lexify.io
- **Phone:** +41 76 232 66 83

Follow Us

Stay updated and connected with us on social media for the latest news, insights, and updates:

- **LinkedIn**: Lexify

Explore More

Visit our website to discover more about our products, services, and the solutions we offer at https://www.lexify.io/