ESMA’s Supervisory Briefing on the authorisation of crypto-asset service providers

June 2025

The relatively recent publication of Regulation (EU) 2023/1114 on markets in crypto-asset[1] (MiCA) in 2023, its innovative nature and the technical complexity in crypto-asset trading has led to the extension of the development stage of the level two and level three regulation that detail and clarify certain obligations and requirements included in the Regulation.

The Supervisory Briefing hereby breaks down part of the content laid out in the MiCA regulation and facilitates its practical implementation. Specifically, it provides National Competent Authorities (NCAs) with guidance aimed at ensuring that authorisation procedures of crypto-asset service providers (CASPs) in the European Union (EU) are governed by common requirements to favour supervisory convergence.

Likewise, these recommendations are also intended to serve companies who wish to provide crypto-asset services in the EU, as they detail those elements that will be required by supervisors in their authorisation and supervision processes. The approach taken in said processes is based on the risk level created by the specific services and nature of each CASP.

[1] 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, (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

Pregunta
What is the purpose of the Supervisory Briefing?

Respuesta
The aim is to standardise and unify the requirements for CASPs to be listed as authorised entities in order to provide services in the EU.

Pregunta
Who is the target audience of the Supervisory Briefing?

Respuesta
NCAs. However, it also contains relevant information for those companies who wish to provide crypto-asset services in the EU under MiCA, as they are required to apply for authorisation to do so.

Pregunta
What is the Supervisory Briefing content?

Respuesta
Overall, it includes several recommendations for NCAs, based on the risks that determine the level of scrutiny

to which companies who wish to be authorised as CASPs in the EU must be subject to. It also sets out guidelines that imply specific requirements to mitigate risks related to the autonomy, governance and outsourcing of certain services to be supervised together with the general principles for the supervision of third-party risks under Regulation (EU) 2022/2554 on digital operational resilience for the financial sector[2] (DORA).

[2] 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. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

Pregunta
Why is ESMA paying special attention to risk factors?

Respuesta
Because it is part of ESMA's policy to base market supervision on the risks that different factors entail, not only to ensure its goal to have stable and efficient markets, but also investor protection. The very nature of CASPs' business and the specificities of crypto-asset markets (a global market in which services are often outsourced and subject to the risks inherent to businesses in which the technological component is part of their essence) means that ESMA considers there are no low-risk CASPs as, their counterparties are often retail investors who lack the experience and knowledge of the institutional ones, additionally the crypto-asset business involves a series of innovative activities that were unregulated until very recently and entail a technical complexity absent so far in traditional financial markets.

Pregunta
What are the main factors that pose a higher risk?

Respuesta
Factors to be considered in order to determine whether the authorisation of CASPs requires a higher degree of scrutiny are as follows:

1. **Size of CASPs**, regarding the number of clients and the amount of assets traded. CASPs with over 1,000,000 annual active users in the EU or a balance sheet exceeding 3,000,000,000 euros should be subject to a higher level of scrutiny, as should smaller entities where NCAs deem appropriate.
2. **The complexity of the group structure and allocation of responsibilities** within the CASP, which should be clear to the supervisor.
3. **Cross-border activity carried out by CASPs.** In order to establish more strict controls, a threshold of over 200,000 active users outside the home Member State is set.
4. **Role in the ecosystem.** Trading platforms and custodians providing services to other CASPs, or whose trading activity could have an impact on the market in the event of an incident, should also be subject to a greater degree of supervision.
5. **Combination of crypto-asset services.** The greater the number of services CASPs intend to provide, the stricter and more exhaustive the supervision.
6. **Business models that involve the combination of activities,** for example, CASPs acting as such and as an issuer of asset-referenced tokens or e-money tokens.
7. **Outsourcing of core functions.**
8. **Supervisory records** available to the European Supervisory Authorities (ESAs), which is not limited to that of the CASP, but also to those of its parent company, branches, shareholders and of those who perform key functions in them.

Pregunta
What key requirements regarding the autonomy and governance of CASPs should be considered?

Respuesta

1. **Sufficient local autonomy subject to the proportionality principle**

   CASPs must have sufficient powers to make autonomous decisions in the EU. To that end, NCAs of home Member States must ensure that CASPs have sufficient staff in their jurisdictions and that at least one executive member of the board of directors resides in said jurisdiction.

   Persons holding relevant positions, or with management responsibilities, should be at the disposal of the relevant NCA without the need for representatives or delegation of powers. In addition, where CASPs have staff working outside the country that issued the authorisation, continuity and regularity in the provision of services should be guaranteed. In any case, key positions should be mainly based in the country granting authorisation to the CASP.

2. **Internal control functions**

   CASPs are responsible, at all times, for compliance and risk management functions. For smaller CASPs, or those with a lower risk profile, risk management and compliance functions can be combined should keeping them separate be disproportionate. On the other hand, the combination of risk management or compliance functions with internal audit functions should be subject to a high level of scrutiny by NCAs.

   These three functions (internal control, risk management and internal audit) should rely on a framework of specific policies and control mechanisms, subject to periodic review.

   Additionally, an adequate internal control framework requires a well-defined structure in which entities staff's roles and responsibilities are clear. At least, one executive member of the board of directors should be appointed as responsible for this internal control framework.

3. **Risk management policy**

   The following elements should be included:

   a. Clear definition of roles and responsibilities of the entity's key staff.
   b. Alignment between the level of risk appetite and the entity's strategic objectives.
   c. For all crypto-asset services, the identification of risks related to integrity, information and communication technology (ICT), operational, market, legal, compliance and conflict of interest. CASPs should keep a risk register.
   d. Use of quantitative and qualitative methods for risk assessment.
   e. Specific actions and mitigation strategies that allow to monitor and reduce exposure to specific risks.
   f. Periodic reports for management bodies and comprehensive assessment of risk management.

4. **Regulatory compliance functions**

   The following elements should be included:

   a. Definition of roles and responsibilities. CASPs must assign at least one person for this role, unless deemed disproportionate given the entity's activity, in which case said role may be combined with risk management tasks.
   b. An annual compliance plan.
   c. Compliance risk follow-up and drafting periodic reports issued for the Executive Committee.
   d. Periodic evaluation, at least once a year, of the effective exercise of this function.
   e. Compliance with European Banking Authority's (EBA) Guidelines on the prevention of

money laundering and terrorist funding.

Pregunta
What are the principles that should guide outsourcing of functions in CASPs?

Respuesta
Under no circumstances should outsourcing agreements involve delegation of functions or services to the extent that CASPs become letter-box entities.

Specifically, ESMA requests analysing the number of outsourced functions and their importance (e.g. whether they are critical for the entity's operation). In making this assessment, ESMA states that NCAs could consider whether these functions represent a relevant percentage of CASPs' total costs. Functions related to non-management IT and human resources support shall not be considered crucial in assessing CASPs' autonomy.

On the other hand, these entities must always have control over the outsourced activity, without the possibility of delegating their responsibilities. Moreover, outsourcing to other jurisdictions should not pose difficulties for NCAs to perform their supervisory duties or prevent them from collecting information from the outsourced entity.

Outsourcing of clients' assets custody should only take place if carried out to entities authorised under MiCA or to those operating under a national authorisation during the grandfathering period.

ICT-related outsourcing requires compliance with DORA.

Pregunta
How should fit and proper assessments of CASPs' board members be carried out?

Respuesta
Fit and proper assessment of managers shall be subject to more thorough controls in the case of larger, more complex and market-relevant CASPs. In doing so, NCAs will consider ongoing criminal proceedings, prior cases of non-compliance by such persons, as well as the possibility of making up for having less crypto-asset knowledge and skills in relation to the rest of the staff.

Link of interest:

Supervisory Briefing: Authorisation of CASPs under MiCA