



Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem

Central Bank of Ireland

MiCAR Authorisation and Supervision Expectations

December 2024

Table of Contents

Introduction.....	3
Our Risk Appetite	3
Central Bank Engagement Principles.....	5
Central Bank Authorisation / Supervisory Expectations..	5
Central Bank’s MiCAR Expectations.....	6
Governance and Accountability.....	7
Protection of Client Assets	8
Business Model and Financial Resilience.....	9
Operational Resilience.....	10
Ownership.....	11
Conflicts of Interest	12
Crisis Management.....	12
Conduct and Transparency.....	13
Anti-Money Laundering (‘AML’)/Countering the Financing of Terrorism (‘CFT’)	14

Introduction

The Central Bank of Ireland (the 'Central Bank') is publishing its supervisory and authorisation expectations for firms seeking authorisation to provide crypto asset services under Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets ('MiCAR'). This document should be read in conjunction with the Central Bank's 2024 "[Guidance on expectations for applicant firms seeking authorisation from the Central Bank to operate as a regulated Firm](#)" ("the Cross Sectoral Guidance").

This document applies to issuers of Asset Referenced Tokens, issuers of Electronic Money Tokens as well as applicant firms seeking authorisation as a Crypto Asset Service Provider ('CASP'), except where indicated.

The Central Bank's intent is that there is clarity, transparency and predictability for applicant firms seeking authorisation, while maintaining the high standards the public expects for regulated providers of financial services. Authorisation is an important part of the gatekeeping role of the Central Bank. This role requires the Central Bank to assess firms' proposals against applicable regulatory standards and legal requirements. Firms that demonstrate that they have met and will continue to meet those standards and requirements can reasonably look to be authorised in a timely manner.

This guidance document is not intended to replace or override any legislative provisions. The Central Bank may update or amend this guidance from time to time, as appropriate.

Our Risk Appetite

The Central Bank's mission requires us to ensure that the financial system operates in the best interests of consumers, investors and the wider economy. Consumer and investor protection risks are inherently high in some crypto activities.

The Central Bank has an agreed MiCAR Risk Appetite that guides our approach when authorising and supervising issuers and CASPs under MiCAR. This risk appetite has been informed by:

- The MiCAR legislative package;
- Existing Authorisation and Supervisory Expectations;
- Our learnings from engaging with firms with crypto related business models to date;
- The external environment and the risks that have crystallised e.g. FTX;
- The product offerings and utility; and
- Engaging with NCAs as well as International and European regulatory authorities

Our assessments of MiCAR authorisation applications will be guided through many perspectives including the use case and utility, suitability, and the risks associated with a crypto product or service. Whether the crypto product that is issued or offered is backed by a reserve of assets or otherwise structured to reliably meet expectations, is fundamentally important. Regarding services, the target customer and investor base, and whether it is retail focused or aimed at institutional clients, is key in shaping our view of risk. We also consider the viability and sustainability of the business model of the crypto issuer or service provider. Where we see higher inherent conduct and investor protection risks in the products offered to customers and investors, we will have higher expectations of a firm's ability to manage these risks.

We expect applicant firms to be fully transparent on all MiCAR activity they intend to undertake, both in the short term and in so far as is possible in the medium to long-term and if their intent is to enter new markets.

Authorisation assessments are conducted on a case-by-case basis, with the nature, scale and complexity of an application being a major consideration both in the focus of the assessment, and the overall application of proportionality within the assessment. For existing authorised/registered firms seeking a MiCAR authorisation, the Central Bank will, as part of its assessment, utilise its supervisory knowledge of the firm. However, there are no predetermined authorisation assessments and all firms currently providing crypto services in Ireland will need to clearly demonstrate to the Central Bank that they

meet all of the new requirements under MiCAR. Through the authorisation process, the Central Bank is seeking to establish whether a firm can meet our supervisory expectations if authorised. Where a firm does not demonstrate that it can meet these expectations, it will not be authorised. Authorisations may be refused based on the criteria set out in Article 21(2) and Article 21(4) for issuers of ARTs and Articles 63(7), 63(8) and 63(10) for CASPs.

Central Bank Engagement Principles

The Central Bank's Engagement Principles are detailed in the [Cross Sectoral Guidance](#).

Applicant firms should read and understand this guidance. The principles are summarised below:

1. Applications should contain up-to-date, accurate and complete information;
2. Applicant firms should make clear statements about the required information. This includes making it clear when information is not available or the applicant does not know the answer;
3. Applicant firms should be well informed of current sectoral and legal requirements;
4. The Central Bank expects applicant firms to be open and cooperative in all of their dealings with us;
5. Applicant firms should include all relevant information of which they are aware regarding their plans, including their projections and plans to add to or alter authorisations or permissions.

Central Bank Authorisation / Supervisory Expectations

The Cross Sectoral Guidance sets out the Central Bank's general expectations of all applicant firms. Applicant firms should read and understand this guidance. The expectations are summarised below:

1. Customer interests are placed at the heart of business models. Securing customer interests, in particular in retail facing business models, needs to be at the centre of a firm's application;
2. Business models should be viable and sustainable;
3. Applicant firms should demonstrate that they have sufficient substance in the State;
4. Applicant firms should demonstrate that they have adequate resources, commensurate to the nature, scale and complexity of their business activities and the risks therein;
5. Applicant firms should evidence governance arrangements commensurate with the nature, scale and complexity of proposed operations;
6. Applicant firms should demonstrate that they have the capability to fully manage any outsourced activities. Firms should ensure they are compliant with the Central Bank's Cross Industry Guidance on Outsourcing¹;
7. Where applicable, applicant firms should evidence suitable arrangements to safeguard customers' funds, which is of paramount importance to the Central Bank;
8. Applicant firms must have robust capital, governance and planning systems in place, in accordance with their individual sectoral requirements, and, therefore, be able to demonstrate and substantiate that they will have adequate and timely sources of funding (including under a plausible but severe stress scenario);
9. Applicant firms must have adequate and sufficient frameworks in place to assess the applicant's compliance risks and to monitor the adequacy and effectiveness of its compliance monitoring processes and its on-going compliance with its legal and regulatory obligations;
10. Applicant firms must be able to demonstrate a clear ownership structure, up to, and including ultimate beneficial owners.

¹ [Cross industry guidance on outsourcing](#)

11. Applicant firms must have a robust framework in place to effectively identify and manage risks relating to ESG and to ensure that the disclosure made to investors is clear and not misleading in terms of sustainability credentials;
12. Applicant firms should demonstrate the ability to recover critical or important business services from a significant unplanned disruption, while minimising impact and protecting their customers and the integrity of the financial system. Applicant firms should ensure they are compliant with the Central Bank's Cross Industry Guidance on Operational Resilience²;
13. Applicants should have plans in place to ensure that it can exit the market in a safe and orderly manner.

Central Bank's MiCAR Expectations

- The Central Bank encourages potential applicant firms to engage early in relation to their business proposal. In this regard, such firms should consider initially engaging with the Central Bank's Innovation Hub³. The Innovation Hub supports responsible innovation by engaging with eligible innovators and providing informal assistance on matters such as:
 - Requirements under the financial services regulatory frameworks (if applicable);
 - How the Central Bank authorise and supervise under these frameworks (e.g. how to obtain a licence);
 - Potential regulatory issues that should be considered; and
 - Referrals to other business teams within the Central Bank, where appropriate.
- Applicant firms should ensure that all submissions are of an appropriate standard, and have obtained all necessary internal/group approvals prior to submission.
- Applicant firms, particularly those proposing significant levels of passporting or outsourcing, should detail the rationale for seeking authorisation in Ireland.

² [Operational resilience and cyber guidance](#)

³ See Introduction section. Further details can be found at <https://www.centralbank.ie/regulation/innovation-hub>

- Applicant firms must consider whether the proposed business model requires more than one type of licence, and take the appropriate steps to seek the required authorisations. In such cases, applicant firms should consider prior to engagement, inter alia, the different legal and regulatory requirements applicable to the authorisations required, and have a comprehensive understanding of same. In addition, where it is proposed that one firm will hold all of the required authorisations, applicant firms should ensure that applications are submitted in a manner that facilitates a holistic assessment of the firm by the Central Bank.

Governance and Accountability

Firms must demonstrate substance and autonomy in Ireland and be led by a local crypto-competent executive and Board with a strong understanding of the local regulatory environment. Firms must maintain robust governance and risk management arrangements.

Applicant firms should:

- Maintain sound and effective governance arrangements, which are commensurate with the nature, scale and complexity of proposed operations, product offering and enterprise wide risks, in particular conduct risk;
- Demonstrate⁴ that Pre-Approval Controlled Function ('PCF') role holders are of good repute, hold the necessary crypto knowledge, skills and experience, and have sufficient time, to perform the role;

⁴ Including through provision of evidence of due diligence conducted by the applicant firm. Applicant firms should also note the final report ["On Joint EBA and ESMA Guidelines on the suitability assessment of members of management body of issuers and on Joint EBA and ESMA Guidelines on the suitability assessment of shareholders and members, whether direct or indirect, with qualifying holdings in issuers of asset-referenced tokens and in crypto-asset service providers."](#)

- Demonstrate⁵ that members of the management body have not been convicted of offences relating to money laundering or terrorist financing or of any other offences that would affect their good repute;
- Demonstrate that the Board has full oversight of the firm and its risks and is of sufficient size, expertise and independence to achieve that outcome;
- Demonstrate local autonomy (including that the Board operates and makes decisions independently from any Group Board), and that close links (between the local entity and another person/entity) do not exist which would impact on the Central Bank performing its supervisory mandate, should the firm be authorised.
- Have a clear organisational structure in place with well-defined, consistent lines of responsibility;
- Have effective processes to identify, manage, monitor and report risks, as well as adequate internal control mechanisms and practices that are consistent with, and which promote, effective risk management; and
- Have a strategy and execution plan with measurable actions to embed a customer centric culture.

Protection of Client Assets

The local firm must have full control of all client assets with robust segregation and prompt access to the reserve assets to meet redemption demands.

Applicant firms should demonstrate that:

⁵ Including through provision of evidence of due diligence conducted by the applicant firm. Applicant firms should also note the final report ["On Joint EBA and ESMA Guidelines on the suitability assessment of members of management body of issuers and on Joint EBA and ESMA Guidelines on the suitability assessment of shareholders and members, whether direct or indirect, with qualifying holdings in issuers of asset-referenced tokens and in crypto-asset service providers."](#)

- The local firm is in full control of all client assets and associated safeguarding accounts;
- A Head of Client Asset Oversight is appointed;
- A safeguarding framework with robust reconciliation and internal control mechanisms and detailed policies and procedures is maintained. The framework must be compliant with regulatory requirements, reflect safeguarding best practice and ensure investors' ownership rights are protected and customer assets are fully segregated;
- A conflicts of interest assessment should be completed annually and reviewed by the Board to ensure that no risks are posed to client assets through the nature and extent of the firm's activities;
- Sufficient safeguarding expertise exists within the Board, in particular the non-executive cohort, to ensure strong independent oversight;
- Robust procedures, systems and controls to manage the risks associated with any outsourcing arrangements are maintained; and
- Independent third party assurance is provided on an annual basis confirming that the safeguarding framework is operating as described and is compliant with regulatory requirements and expectations. For initial authorisation, this assurance may also be required.

Business Model and Financial Resilience

Firms must maintain a board approved business strategy which demonstrates the viability and sustainability of the business model and which fully reflects the vulnerabilities stemming from the product offering.

Applicant firms should:

- Demonstrate through a financial plan the key drivers of profitability and how the firm can remain financially resilient in stress, in particular, an event driving significant volatility in the crypto market. Key assumptions underpinning the financial plan, including macro-economic variables, should be included;
- Maintain a strong capital management framework, which quantifies potential capital deterioration from enterprise wide risks (scrutiny will be placed on the sources of capital for the first three years of operation);
- Where they belong to a group, provide an explanation of group activities and how the activities of the firm will fit within the group strategy and interact with the activities of the other entities of the group; and
- Ensure their risk appetite is aligned with, and embedded in, the firm's business strategy in a way that it can be assessed both qualitatively and quantitatively, and ensure that it is appropriately communicated across the firm.

Operational Resilience

Firms must ensure continuity and regularity in the performance of their services including Distributed Ledger Technology (DLT) and Blockchain.

Applicant firms should:

- Demonstrate that robust plans are in place to ensure continuity and regularity in the performance of the applicant's activities;
- Demonstrate that, where outsourcing arrangements are in place, the firm maintains full risk ownership and a detailed operational understanding for all aspects of its activities including DLT;
- Outsourcing or delegation arrangements, under which entities confer either a substantial degree of activities or critical functions to other entities, should not result in those entities becoming letterbox entities;

- Such concerns are heightened where the outsource service provider is located outside the EU, as the ability of firms and the Central Bank to, respectively, control and supervise may be significantly impacted;
- Maintain robust documentation and oversight of the Information and Communications Technology (ICT) systems and DLT infrastructure relied upon, where relevant, and on the security arrangements;
- CASPs and issuers of Asset Referenced Tokens are subject to DORA and the specific technical requirements set out in MiCAR. DORA sets out a new EU framework for managing ICT risks in the financial sector. The new rules impose a number of obligations on all financial institutions and their critical third-party ICT services providers. DORA aims to consolidate and update ICT risk management requirements, currently held separately in various legal acts. It sets up a comprehensive framework in areas such as:
 - ICT risk management;
 - ICT incident management;
 - operational resilience testing; and
 - management of third-party ICT service providers.

Ownership

Firms must ensure a full, transparent and corroborated view of the identity of direct and indirect shareholders as well as any party, which can exercise significant influence. Ownership and operating structures must be designed to achieve maximum transparency and clarity as to the ownership of the firm.

Applicant firms should:

- Provide a full and transparent view of the identity of all direct and indirect shareholders (qualifying or otherwise) as well as any party that can exercise significant influence over the applicant;

- Demonstrate⁶ that shareholders are of good repute and have not been convicted of offences relating to money laundering or terrorist financing or of any other offences that would affect their good repute; and
- Ensure that submissions are supported by all necessary corroborating documents.

Conflicts of Interest

Firms must ensure that no risks are posed to customer interests through conflicts of interest and that a robust system is in place which can proactively identify and subsequently remedy any conflicts in a timely manner.

Applicant firms should:

- Maintain policies which are commensurate with the nature, scale and range of crypto-asset and other services that the firm intends to provide, and of the other activities of the group to which it belongs (if applicable);
- Maintain policies, which ensure that conflicts of interests can be identified and subsequently remedied in a timely manner. Annual board attested assessments are to be completed; and
- Ensure that remuneration policies, procedures and arrangements do not create conflicts of interest.

Crisis Management

Firms must maintain detailed plans appropriate to support an orderly wind-down of their activities and timely redemption of customer funds without causing undue economic harm to their customers.

⁶ Including through provision of evidence of due diligence conducted by the applicant firm.

Applicant firms should maintain:

- Detailed plans appropriate to support an orderly wind-down of their activities and timely redemption of customer assets without causing undue economic harm to their customers; and
- Recovery plans that include appropriate conditions and procedures to ensure the timely implementation of recovery actions where a firm experiences an issue of non-compliance.

Conduct and Transparency

Firms must demonstrate how customers' interests are secured and how the suitability of their product offering is being proactively assessed in accordance with customers' risk tolerance.

Applicant firms should:

- Maintain a Business Standards Plan outlining standards for the purpose of ensuring that in the conduct of its affairs a firm (a) acts in the best interests of customers and of the integrity of the market, (b) acts honestly, fairly and professionally, and (c) acts with due skill, care and diligence;
- Ensure that sufficient information is provided to customers on each product offering in a comprehensive, clear, accurate, not misleading and understandable manner for the intended audiences of customers, and other relevant stakeholders and investors;
- Note that the Consumer Protection Code applies to regulated firms providing regulated activities to individuals and small businesses within the State. A regulated firm means a financial services provider authorised, registered or licensed by the Central Bank or other EU or EEA Member State that is providing regulated activities. Once in effect, firms that fall under MiCAR, will subsequently

be subject to the requirements of the Consumer Protection Code where appropriate;

- Ensure that business models are aligned with the relevant crypto-asset white paper(s), without contradictions between what is set out in the programme of operations and the information included for public disclosure to potential token holders;
- In the interests of investor protection, as well as to promote an effective system of internal governance, provide their clients with easy access to a clear, understandable and up-to-date description of their complaints-handling procedure; and
- Maintain effective arrangements, systems and procedures to prevent and detect market abuse.

Anti-Money Laundering ('AML')/Countering the Financing of Terrorism ('CFT')

Applicant firms must demonstrate that strong risk management practices and internal controls are in place in order to identify, assess and manage risks, including money laundering and terrorist financing risks and financial sanctions risks. Applicant firms must ensure compliance with the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended) and all relevant Financial Sanctions legislation.

Applicant firms should:

- Carry out an AML/CFT risk assessment of their business;
- Undertake customer due diligence of their customers;
- Carry out ongoing monitoring of customers and customer transactions;

- File Suspicious Transaction Reports with the Financial Intelligence Unit Ireland and the Revenue Commissioners in instances where money laundering or terrorist financing is known or suspected;
- Maintain and implement AML/CFT policies, procedures and controls;
- Retain appropriate records;
- Provide AML/CFT training to all staff on an ongoing basis;
- Implement and maintain appropriate and effective Financial Sanctions controls; and
- Where appropriate freeze assets of sanctioned individuals/entities.

Further information in relation to the Central Bank's expectations in relation to AML/CFT can be found on the website.

Further information in relation to common EU standards on the governance arrangements and the policies, procedures and controls financial institutions should have in place to be able to comply with Union and national restrictive measures can be found on the [EBA website](#).

Error! Unknown document property name.

T: +353 (0)1 224 5800
E: publications@centralbank.ie
www.centralbank.ie



Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem