Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Guidance Note for Crypto-Asset Service Providers – Key Facts Document

Under Regulation (EU) 2023/1114 (Markets in Crypto Assets Regulation) ("MiCAR")

November 2024

Contents

Central Bank Authorisation Assessment Process – Crypto Asset Service Providers

Applicant firms seeking authorisation must clearly demonstrate that they can meet the applicable regulatory obligations and the Central Bank of Ireland's ("Central Bank") supervisory expectations both at the point of authorisation and post authorisation. The authorisation process consists of the two phases, with a number of stages within each stage:

1. **Pre-Application Phase:** This consists of two stages:
   - Initial meeting with the applicant firm; and
   - Submission of a Key Facts Document (KFD).

2. **Application Phase:** This consists of the following stages:
   - Submission of formal application seeking authorisation under MiCAR to the Central Bank;
   - Assessment of completeness of application by the Central Bank;
   - Assessment of application by Central Bank; and
   - Communication of decision to the applicant firm: granting or refusing authorisation as a crypto-asset service provider.

Purpose of the Guidance Document

The Key Facts Document ("KFD") provides the Central Bank with high-level information in respect of the applicant Crypto-Asset Service Provider's ("CASP") proposed business and operational model and associated risks, including details in respect of the applicant firm's background, ownership, number and type of clients, capital projections, governance and staff resourcing arrangements and outsourcing arrangements. Please note that the KFD stage does not constitute the formal assessment (which commences once a formal application is submitted).

The purpose of this Guidance Note is to set out the Central Bank's expectations regarding the content of the KFD to be submitted.

The purpose of the KFD is two-fold:

(i) to facilitate the Central Bank in obtaining a clear, high-level understanding of the applicant firm's proposed business model, risks and governance arrangements; and
(ii) to enable the Central Bank to identify, where possible, potentially material issues in respect of the applicant firm's proposal, at an early juncture, to allow timely feedback be provided to the applicant firm.

Expectations

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 applicant 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 an applicant firm can meet our supervisory expectations if authorised. Where an applicant 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 Articles 63(7), 63(8) and 63(10) for CASPs.

The Central Bank's engagement principles and general expectations in terms of authorisation are detailed in the 'Guidance on expectations for applicants seeking authorisation from the Central Bank of Ireland to operate as a regulated Firm'. Applicant firms should read and understand this guidance.

Key areas of focus for the Central Bank, in terms of the authorisation and supervision of CASPs, are:

- Independence and Autonomy of the applicant firm (within a group structure);
- Governance and Accountability;
- Protection of Client Assets;
- Business Model and Financial Resilience;
- Operational Resilience;
- Ownership of the applicant firm;
- Conflicts of Interest;
- Crisis Management;
- Conduct and Transparency;
- Anti-Money Laundering ('AML')/Countering the Financing of Terrorism.

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 if their intent is to enter new markets.

Expectations for KFD Stage

The Central Bank expects that the potential applicant firm takes under consideration all items discussed and feedback provided during the pre-application engagement, making any changes required to meet the Central Bank's expectations prior to submitting the KFD. During the KFD process, potential applicant firms should expect engagement with the Central Bank to address any questions and provide any clarifications sought on the proposal. The Central Bank expects applicant firms to engage constructively and in a timely manner with the CASP Authorisation Team during this process.

At the conclusion of the KFD stage, the Central Bank may provide feedback on further elements of the proposal that the Central Bank will require the applicant firm to consider and reflect in the formal application; or the Central Bank may provide the applicant firm with feedback on material item(s) which it deems necessary for the applicant firm to consider and address before the applicant firm submits a formal application.

Where further work is required by applicant firms to progress to the formal application stage, the Central Bank will provide clear and specific feedback to the applicant firm in line with its commitment to provide an open and transparent application process.

The Central Bank does not anticipate that the KFD process is an open-ended process. There is a limit to the time spent and number of engagements. In general, high quality KFD submissions progress more efficiently, as there is likely to be fewer questions and clarifications required. It is important that the KFD provides sufficient detail to enable the Central Bank to identify any potential issues or concerns that may impede the progression of a proposed application.

The Central Bank expects applicant firms to have a full awareness and understanding of the relevant governing legislation, regulatory definitions, regulatory guidelines, and regulatory technical standards applying to CASPs prior to submitting a KFD. If appropriate, applicant firms are advised to seek professional advice from subject matter experts to assist in this stage of the authorisation process.

Guidance on Completing the KFD

For each section, the applicant firm should provide any information or documentation requested. In the event that a section does not apply, the applicant firm must provide an explanation as to why it considers this to be the case.

For each section, where separate and distinct documentation is requested, applicant firms should ensure that these documents, along with any other accompanying documents, are clearly marked and referenced in accordance with the relevant section.

Where possible, information provided should be in Microsoft Word (or equivalent) format rather than scanned versions.

All documentation should be submitted using Kiteworks, a secure file sharing mechanism used by the Central Bank. When submitting any documentation, please contact the CASP Authorisation Team at CASPAuthorisations@centralbank.ie to request Kiteworks access.

1. Background

Provide details on the applicant firm's background to include the following information:	
(i) Introduction	Introduce the applicant firm and provide details in respect of the purpose, scope and rationale for the authorisation application.
(ii) Background to Applicant firm	A brief description of the applicant firm. Details should, at a minimum, include the following: • Type of legal entity (e.g. private legal entity etc.); • Incorporation status; • Location of head office; • The reason(s) why the applicant firm has selected Ireland as a location from which to carry out crypto-asset services; • Whether the applicant firm has applied for or is seeking a MICAR authorisation in any other jurisdiction; and • Whether any previous applications for authorisation/ licensing/ registration have been refused or withdrawn.

2. Business Model

Provide a description of the applicant firm's proposed business and operational model. Details should at a minimum include the following:	
(i) An Overview of the Business Model of the Applicant Firm	• A description of the business model, strategy and unique value proposition of the applicant firm; • A description of the operating model of the applicant firm; • The proposed customer base, including the forecast number of clients, type of clients and their geographical location for each of the first three years of operation and the rationale and basis for the applicant firm's estimates and variations year on year; • The expected number and type of clients, volume of orders, transactions and expected amount of crypto-assets under custody for each of the first three years (if applicable); • An overview of the applicant firm's proposed revenue model setting out the individual revenue lines and fee structures; and

	• The planned marketing and promotional activities for the proposed crypto-asset services including location of marketing activities.
(ii) Details of the Services to be Provided	A clear and detailed description of proposed activities (in a coherent and unambiguous manner) – distinguishing between regulated, unregulated activities and ancillary/other activities. This should include, at a minimum: • An outline of the crypto-asset services, as defined under Article 3(16) of MiCAR, that the applicant firm intends to provide and the types of crypto-assets to which the services will relate; • For each proposed service/transaction type, involving funds flows, please submit detailed funds flows diagrams and/or process flow charts; • A description of other unregulated crypto-asset services the applicant firm intends to provide; • A description of other regulated/unregulated services the applicant firm intends to provide; and • Confirmation on whether the applicant firm intends to offer crypto-assets to the public or seek admission to trading of crypto-assets and if so, of what type of crypto-assets.
(iii) Details of the Group, where applicable	Where the applicant firm is part of a Group, please provide: • A Group structure chart including detail of the applicant firm ownership (see Appendix II for the template to be completed); • The geographical location of all group entities and details of the activities undertaken; • Details as to how the Group generates its revenue; • Details of any Group entities that are/have been authorised and regulated by other competent authorities;

	• Details on how the activities of the applicant firm will fit within the Group strategy and interact with the activities of the other entities of the group; and • Information in relation to any investment in any other crypto-asset firms by Group entities.
(iv) Financial Viability	See Section 3 (i) – Capital Requirements. The information submitted regarding section 3(i) should be clearly marked and referenced to this section.
(v) Outsourcing Arrangements[1]	An overview of the applicant firm's outsourcing arrangements (see table at Appendix I for details required) including: • A high-level narrative in respect of the proposed third party and/or intra group outsourcing arrangements, where applicable; • Overview of the nature, scale and rationale for all outsourcing activities should be provided, including details in respect of the proposed Outsourced Service Providers ("OSPs"), confirmation that contractual arrangements (e.g. Service Level Agreements) with each OSP are/will be in place and a summary of the governance, management and oversight arrangements in respect of outsourced activities etc.; • The applicant firm should include a table indicating, for each outsourced function, the nature of the outsourcing (critical/non-critical), the name and location of the relevant OSP, the number of FTE that the relevant OSP has available/dedicated to the applicant firm, the responsible executive in the applicant firm in terms of oversight of the outsourced functions and whether sub-

[1] Please provide overview of ICT related outsourcing in this section with further detail provided in Section 8 ICT Systems and Security Arrangements.

	outsourcing applies (see Appendix I for the template to be completed); • The applicant firm should provide details on how it is satisfied/will be satisfied that it is fully compliant with the relevant outsourcing requirements, including, but not limited to, the requirements set out in Article 73 of MiCAR, the EBA Guidelines on Outsourcing Arrangements and the Central Bank's Cross-Industry Guidance on Outsourcing; • If the applicant firm relies on the Group's systems and processes, it should clearly articulate how these systems and processes work holistically, and confirm that the systems and processes are compliant with the EU/Irish regulatory requirements; and • Details of the applicant firm's internal control arrangements to ensure effective and appropriate oversight over crypto - asset activities which are outsourced to a third party, including any Group entity.
(vi) Risk Framework	An overview of the applicant firm's risk management framework including: • Scope, remit and resources of risk management function; • High-level overview of the risk management framework in place; • Applicant firm's key risks arising from the proposed service offerings, to include assessment, monitoring and mitigation; • A copy of the firm-specific Risk Appetite Statement which is aligned with the applicant firm's business strategy; and • A copy of the applicant firm's Risk Register.

3. Capital Requirements

Demonstrate how the applicant firm will be in a position to meet its capital requirements over the first three years of operation. Details should at a minimum include the following:	
(i) **Financial Viability**	Financial projections for the first 3 years of operations post-authorisation. The applicant firm should demonstrate how it will be in a position to meet its applicable regulatory capital requirements over the period including in stress scenarios. Financial information required[2]: • Projected Profit and Loss Accounts for each of the first 3 Years; • Projected Balance Sheet for each of the first 3 Years; • Projected Regulatory Capital, Own Funds Requirements and Operational Funding Levels for each of the first 3 Years; • Information (quantitative and/or qualitative) on drivers of profitability and revenue; • Sources of Regulatory and Share Capital/Funding; • Assumptions used to form projections; • Where the applicant firm is operational, please also provide the approved (where audited) financial statements from the last three years; • Where applicable, provide projected Profit and Loss Accounts and projected Balance Sheet at consolidated group and sub-consolidated level for each of the next 3 years.
	The amount of Own Funds covered by an insurance policy or guarantee, details of the provider and a copy of the proposed policy evidencing the characteristics and risk coverage of the agreement.
	Information in relation to the capital management/monitoring framework which, inter alia, quantifies potential capital deterioration from enterprise wide risks.
	Information on the status of engagement with Credit Institutions regarding the provision of banking services to the applicant firm.

[2] Detailed financial projections are required covering the first three years of operation including projected income statement, balance sheet and capital requirements in excel format showing all formulas. This should clearly set out all underlying assumptions.

4. Governance

Provide a description of the applicant firm's governance arrangements and internal control mechanisms[3]. Details should, at a minimum, include the following:	
(i) Governance & Staffing	• Proposed composition of the board of directors and proposed board sub-committees e.g. purpose, membership, frequency of meetings, chair etc.; • Proposed executive/other (non-board) committee structures, their composition and purpose; • Organisational chart (see Appendix III) depicting all staff members, including their locations, functional units (e.g. Compliance, Internal Audit, IT, Finance etc.), clear reporting lines within the applicant firm and to other Group entities; • Details of proposed PCF role holders in the applicant firm (where known), including non-executive directors, proof of good repute, knowledge, skills, experience and of sufficient time commitment including whether these individuals have previously been approved by the Central Bank (see Appendix IV for the template to be completed); • Number of proposed employees and FTE, noting where employees are shared across other group entities (see Appendix V for the template to be completed); • Where the applicant firm belongs to a Group, please demonstrate that the Board is independent, can exercise local autonomy and that close links do not exist which would impact on the Central Bank performing its supervisory mandate, should the applicant firm be authorised.
(ii) Ownership	• An organisation chart detailing all shareholders of the applicant firm, both direct and indirect, qualifying or otherwise as well as any party that can exercise significant influence over the applicant firm (see Appendix II for the template to be completed). This should indicate the percentage shareholding of each shareholder. • Confirm that for all shareholders and members, that have qualifying holdings in the applicant firm, the absence of a criminal record in respect of convictions or penalties imposed under the applicable commercial law, insolvency law and financial services law in relation to anti-money laundering and counter-terrorist financing, fraud or professional liability.

[3] Applicant firms should note the final report on the Joint EBA and ESMA Guidelines on the suitability assessment of members of management body 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

(iii) Internal Controls	An overview of the applicant firm's internal control arrangements to include: • Independence, scope and remit of the internal control functions; • Nature and frequency of internal control functions' reporting to management body; • A description of the Information and Communication Technology (ICT) systems, safeguards and controls put in place to monitor the activities of the applicant firm.

5. Detection and prevention of money laundering and terrorist financing

(i) Registered VASPs	For applicant firms registered as a VASP, these firms should confirm that there have been no changes to both the business model (nature, scale and complexity) and the AML/CFT Framework. If there have been changes, the applicant firm must highlight the changes and set out the rationale for any such changes.
(ii) New applications	• If the applicant firm is not registered as a VASP, it should submit a summary of its proposed AML & CFT Framework including how it will ensure compliance with the provisions of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended).

6. Conduct and Conflicts of Interest

Provide a description of the applicant firm's conduct & transparency and conflict of interest arrangements. Details should, at a minimum, include the following:	
(i) Conduct & Transparency	• A description of the applicant firm's complaints handling procedure; • The applicant firm's 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; • Where relevant, please provide a description of the arrangements and market surveillance operations put in place to prevent and detect market abuse applicable to your business activities.
(ii) Conflicts of Interest	• A copy of the applicant firm's Conflicts of Interest Policy and details on how the applicant firm identifies, monitors and mitigates conflicts of interest;

	• Demonstrate how the policy is commensurate to the scale, nature and range of crypto-asset services that the applicant firm intends to provide and of the other activities of the Group to which it belongs (if applicable); • Include any potential or actual conflicts of interest in relation to any investments in other crypto-asset type firms within the Group or outside the Group.

7. Business Continuity & Wind-down

Provide a description of the applicant firm's business continuity and wind-down arrangements. Details should at a minimum include the following:	
(i) Business Continuity Arrangements	An overview of proposed business continuity arrangements supported by the applicant firm's business continuity plan. The description should include: • The critical functions of the applicant firm; • The steps to be taken to ensure continuity; • Scenarios that would lead to invocation of the Business Continuity Plan; • Monitoring arrangements; and • Business continuity testing arrangements.
(ii) Wind-down Arrangements	An overview of proposed wind-down arrangements supported by the applicant firm's wind-down plan. The description should include, at a minimum: • The governance and escalation process; • Wind-down steps; • Scenarios that would lead to invocation of the Wind Down Plan; • Non-financial resources required to carry out the wind down steps; and • Stakeholder impact assessment.

8. ICT Systems and Security Arrangements

From January 2025, the Digital Operational Resilience Act (DORA) is applicable to CASPs. DORA sets out a new EU framework for managing ICT risks in the financial sector. Applicant firms will observe similarities between a number of key DORA requirements and existing Central Bank guidance in relation to Outsourcing, Operational Resilience and IT & Cybersecurity Risks as well as in existing sectoral guidelines.		
		Confirm Yes or No or where specified provide a narrative
ICT governance, organisation and ICT risk management.	Pursuant to Article 5 of the Digital Operational Resilience Act ("DORA"), has the management body of the applicant firm defined, approved, and will oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework.	**If Yes**, please include a supporting narrative describing how the management body of applicant firm has defined, approved, and will oversee and be responsible for the implementation of all arrangements related to the ICT risk. Please also describe the supporting human resources to ensure that the applicant firm complies with DORA. **If No**, please specify when the management body of the applicant firm will define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework.
	Pursuant to Article 6 DORA, has the applicant firm developed a sound, comprehensive and well-documented ICT risk management framework as part of its overall risk management system to enable it to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience.	**If Yes**, please include a supporting narrative describing how the applicant firm has defined strategies, policies, procedures, ICT protocols and tools necessary to duly and adequately protect all information assets and ICT assets, including computer software, hardware, servers, as well as to protect all relevant physical components and infrastructures, such as premises, data centres and sensitive designated areas, to ensure that all information assets and ICT assets are adequately protected from risks including damage and unauthorised access or usage. This should include an explanation of:

		(a) how the ICT risk management framework supports the applicant firm's business strategy and objectives; (b) the risk tolerance level for ICT risk, in accordance with the risk appetite of the applicant firm and analysing the impact tolerance of ICT disruptions; (c) the relevant security objectives; (d) the ICT reference architecture and any changes needed to reach specific business objectives; (e) the different mechanisms put in place to detect, protect and prevent impacts of ICT-related incidents; (f) how it will evidence the number of reported major ICT-related incidents and the effectiveness of preventive measures; (g) the ICT multi-vendor strategy at entity level showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of third-party service providers; (h) the digital operational resilience testing; and (i) the communication strategy in case of ICT-related incidents. **If No**, please specify when the applicant firm will develop a sound, comprehensive and well-documented ICT risk management framework as part of its overall risk management system.
ICT systems, protocols and tools	Pursuant to Article 7 DORA and in order to address and manage ICT risk, will the applicant firm use and maintain updated ICT systems, protocols and tools that are:	**If Yes**, please provide a narrative describing how the applicant firm will use and maintain updated ICT systems pursuant to Article 7 DORA. **If No**, please specify when the applicant firm will ensure controls are defined in respect of its ICT systems to

	(a) appropriate to the magnitude of operations supporting the conduct of its activities (b) reliable; (c) equipped with sufficient capacity to accurately process the data necessary for the performance of activities and the timely provision of services, and to deal with peak orders, message or transaction volumes, as needed, including where new technology is introduced; (d) technologically resilient in order to adequately deal with additional information processing needs as required under stressed market conditions or other adverse situations.	ensure they will maintained and updated pursuant to Article 7 DORA.
Identification	Pursuant to Article 8 DORA, as part of the ICT risk management framework referred to in Article 6 (1), has the applicant firm identified, classified and adequately documented all ICT-related business functions, the information assets supporting these functions, and the ICT system configurations and interconnections with internal and external ICT systems and has the applicant firm put in place governance controls to review as needed, and at least yearly, the adequacy of the classification of the information assets and of any relevant documentation.	**If Yes**, please provide a narrative describing how the applicant firm, as part of its ICT risk management framework referred to in Article 6 (1), classified and adequately documented all ICT-related business functions, the information assets supporting these functions, and the ICT system configurations and interconnections with internal and external ICT systems and the governance controls to review as needed, and at least yearly, the adequacy of the classification of the information assets and of any relevant documentation. **If No**, please specify when the applicant firm will ensure it will meet the requirements set out in Article 8 DORA.

Protection and prevention	Pursuant to Article 9 (2) DORA, has the applicant firm designed, procured and implemented ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit.	**If Yes**, please provide a narrative describing the ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems. **If No**, please specify when the applicant firm will design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit.
	Pursuant to Article 9 (4) DORA, has the applicant firm defined and documented policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes.	**If Yes,** please provide a narrative describing the policies and protocols for strong authentication mechanisms dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes. **If No**, please specify when the applicant firm will define and document policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes.
	Pursuant to Article 9 (4) DORA, has the applicant firm documented policies, procedures	**If Yes,** please provide a narrative describing the policies, procedures

	and controls for ICT change management, including changes to software, hardware, firmware components, systems or security parameters, that are based on a risk assessment approach and are an integral part of the applicants overall change management process, in order to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner.	and controls for ICT change management. **If No,** please specify when the applicant firm will put in place a documented policies, procedures and controls for ICT change management,
Response and recovery	Pursuant to Article 11 (1) DORA, as part of the applicants ICT risk management framework referred to in Article 6 (1) DORA and based on the identification requirements set out in Article 8 DORA, has the applicant firm put in place a comprehensive ICT business continuity policy through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aimed at: (a) recording all ICT-related incidents; (b) ensuring the continuity of the financial entity's critical functions; (c) quickly, appropriately and effectively responding to and resolving all ICT-related incidents, in particular but not limited to cyber-attacks, in a way which limits damage and prioritises resumption of activities and recovery actions; (d) activating without delay dedicated plans that enable containment measures, processes and technologies suited to each	**If Yes**, please provide a narrative describing the ICT business continuity policy (which should encompass dedicated, appropriate and documented arrangements, plans, procedures and mechanisms). **If No**, please specify when the applicant firm will put in place a comprehensive ICT business continuity policy.

	type of ICT-related incident and preventing further damage, as well as tailored response and recovery procedures established in accordance with Article 12 DORA,; (e) estimating preliminary impacts, damages and losses; (f) setting out communication and crisis management actions which ensure that updated information is transmitted to all relevant internal staff and external stakeholders in accordance with Article 14, and reported to competent authorities in accordance with Article 12 DORA,	
Backup policies and procedures, restoration and recovery procedures and methods	Pursuant to Article 12 (1) DORA, has the applicant firm developed and documented backup policies and procedures which specify the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data including restoration and recovery procedures and methods.	**If Yes**, please provide a narrative describing the backup policies and procedures (which should encompass the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data including restoration and recovery procedures and methods). **If No**, please specify when the applicant firm will develop, document and implement backup policies and procedures.
ICT–related incident management process	Pursuant to Article 17 DORA, has the applicant firm defined and established an ICT-related incident management process to detect, manage and notify ICT-related incidents.	**If Yes**, please provide a narrative describing the ICT-related incident management processes. **If No,** please specify when the applicant firm will define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.

Testing of ICT tools and systems	Pursuant to Article 24 (1) DORA and taking into account the criteria set out in Article 4 (2) DORA, has the applicant firm established, a sound and comprehensive digital operational resilience testing programme as an integral part of its ICT risk-management framework referred to in Article 6 DORA.	**If Yes**, please provide a narrative describing the sound and comprehensive digital operational resilience testing programme and how it has been incorporated into the ICT risk-management framework. **If No**, please specify when the applicant firm will establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework referred to in Article 6 DORA.
ICT third-party risk management	Pursuant to Article 28 DORA has the applicant firm put in place contractual arrangements for the use of ICT services to run their business operations and ensure it will be, at all times, fully responsible for compliance with, and the discharge of all obligations under DORA and are the contractual arrangements on the use of ICT services included pursuant to Article 30 (2) DORA	**If Yes**, please provide a narrative as to how the applicant firm has put in place contractual arrangements for the use of ICT services to run their business operations and how it will be, at all times, fully responsible for compliance with, and the discharge of all obligations under DORA and that the contractual arrangements pursuant to Article 30 (2) DORA are defined within those arrangements. **If No**, please specify when and how the applicant firm will put in place contractual arrangements for the use of ICT services to run their business operations.
	Has the applicant firm: • defined ICT third-party risk management controls including, but not limited to, risk analysis, due diligence, governance frameworks: and • roles and responsibilities to continuously monitor the performance of the third parties including, but	**If Yes,** please provide a narrative as to how the applicant firm has defined ICT third-party risk management controls and roles and responsibilities to continuously monitor the performance of the third parties. **If No,** please specify when and how the applicant firm will define its ICT third-party risk management controls and roles and responsibilities to

	not limited to, intragroup and sub-outsourcing arrangements.	continuously monitor the performance of the third parties.
	If the applicant firm intends to utilise the services of any third party that is providing or supporting critical or important functions please describe the contractual arrangements (identity and geographical location of the providers, description of the outsourced activities or ICT services with their main characteristics and a copy of contractual agreements). See table at Appendix I for details required.	
	If the applicant firm intends to utilise the services of any third party that is providing or supporting custody services, please describe: • How private keys are\will be stored at the third party (hot, warm or cold storage); • How external assurance reports will be performed on the third party • The key management security and authorisation protocols at the third party; • The external third party's data recovery plan, and whether it is regularly tested for reliability.	
ICT supporting systems	Please provide a description of the critical systems and the relevant governance framework, to support the applicant firm's business, including, but not limited to any underlying DLT and/or DLT networks and/or infrastructure, and node management.	
	If the applicant firm is performing custody services, please describe from an ICT perspective: • How private keys are\will be generated, stored and managed (hot, warm or cold storage) including infrastructure used by the applicant firm; • The key management security and authorisation protocols and controls; • How external assurance reports will be performed; and • The applicant firm's data recovery plan and whether it is regularly tested for reliability.	

9. Client Assets

Provide a description of the applicant firm's protection of client assets arrangements. Details should at a minimum include the following:	
(i) Segregation of Client Assets	Describe and, where available, provide supporting evidence as to how • Clients' funds[4] and clients' crypto-assets and clients' wallets are segregated from those of the applicant firm; • The applicant firm segregates clients' crypto-assets from other clients' crypto-assets, including when omnibus wallets are used; • The applicant firm maintains books and records, both on and off chain, in order to achieve segregation and return client crypto-assets in the event of the applicant firm's insolvency. The above description should be comprehensive and include details on hot and cold wallet storage, wallet transfer management, including the transfer of crypto assets between wallets, the payment of on chain transaction fees, and on-chain and off-chain reconciliation procedures.
(ii) Cryptographic Keys	• Describe the approval system for and safeguarding of cryptographic keys.
(iii) Safeguarding of Client Funds	• Where relevant, please describe how client funds, other than e-money tokens, are deposited with a credit institution by the end of the business day following the day on which they were received and are held in an account separately identifiable from any accounts used to hold funds belonging to the applicant firm. Please also outline the process followed by the applicant firm in selecting the credit institutions in which to deposit clients' funds and the frequency of review of this selection.
(iv) Oversight	• Demonstrate how sufficient expertise exists within the Board, in particular the non-executive cohort, to ensure strong independent oversight of the safeguarding and segregation of clients' crypto-assets and funds.

[4] "funds" means banknotes and coins, scriptural money or electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC

10. Providing the Service of Custody and Administration of Crypto-assets on Behalf of Clients

Where the applicant firm intends to provide the service of custody and administration of crypto-assets on behalf of clients, please provide the following information:	
(i) Custody & Administration Arrangements	• A description of the arrangements linked to the type of custody offered to clients; and • A copy of the applicant firm's standard agreement for the custody and administration of crypto-assets on behalf of clients.
(ii) Custody & Administration Policy	The applicant firm's custody and administration policy, including a description of identified sources of operational and ICT risks for the safekeeping and control of the crypto-assets or the means of access to the crypto-assets of clients. This should be supported by: • the policies and procedures, and a description of the systems and controls, to manage those risks, including where the service is outsourced; • the policies and procedures relating to, and a description of, the systems to ensure the exercise of the rights attached to the crypto-assets by the clients; and • the policies and procedures relating to, and a description of, the systems to ensure the return of crypto-assets or the means of access to the clients.
(iii) Client Assets	• Information on how the crypto-assets and the means of access to the crypto-assets of the clients are identified; and • Information on arrangements to minimise the risk of loss of crypto-assets or of means of access to crypto-assets.

11. Operation of a Trading Platform for Crypto-assets

Where the applicant firm intends to operate a trading platform for crypto-assets, please provide the following information:
i. Information as to whether the Trading Platform is part of a larger Group that contains a market maker; ii. Rules regarding the admission of crypto-assets to trading; iii. The approval process for admitting crypto-assets to trading, including the customer due diligence carried out; iv. The list of any categories of crypto-assets that will not be admitted to trading and the reasons for such exclusion; v. Rules regarding suspension of trading and removal of crypto assets for breach of rules by the issuers of crypto assets; vi. Information in relation to basic listing criteria;

vii. Information in relation to Order / Quote transparency;
viii. Information in relation to DEA (Direct Electronic Access) access;
ix. A description of the trading protocol and what types of orders are accepted on the platform;
x. The policies and procedures and fees for the admission to trading, together with a description, where relevant, of membership, rebates and the related conditions;
xi. The rules governing order execution, including any cancellation procedures for executed orders and for disclosing such information to market participants;
xii. The policies and procedures adopted to assess the suitability of crypto-assets;
xiii. The systems, procedures and arrangements put in place to ensure that their trading system is resilient, has sufficient capacity to deal with peak order and message volumes, is able to ensure orderly trading under conditions of severe market stress, is able to reject orders that exceed pre-determined volume and price thresholds or are clearly erroneous, and is able to prevent or detect market abuse;
xiv. The systems, procedures and arrangements to make public any bid and ask prices, the depth of trading interests at those prices which are advertised for crypto-assets through their trading platforms, and also price, volume and time of transactions executed in respect of crypto-assets traded on their trading platforms;
xv. The fee structure and a justification of how it is transparent, fair and non-discriminatory and that it does not create incentives to place, modify or cancel orders or to execute transactions in a way that contributes to disorderly trading conditions or market abuse;
xvi. The systems, procedures and arrangements to keep data relating to all orders at the disposal of the Central Bank of Ireland or the mechanism to ensure that the competent authority has access to the order book and any other trading system;
xvii. Information on the settlement of transactions including whether the final settlement of transactions is initiated on the distributed ledger or outside, the timeframe within which the final settlement of crypto-asset transactions is initiated, the systems and procedures to verify the availability of funds and crypto-assets, the procedures to confirm the relevant details of transactions, the measures foreseen to limit settlement fails, and the definition of the moment at which settlement is final and the moment at which final settlement is initiated following the execution of the transaction;
xviii. Outline the Rulebook notification change periods;
xix. A description of the arrangements, systems and procedures to prevent and detect market abuse.

12. Providing the Service of Exchanging Crypto-assets for Funds or other Crypto-assets

Where the applicant firm intends to provide the service of exchange of crypto-assets for funds or other crypto-assets, please provide the following information:	
(i) Commercial Policy	• A description of the non-discriminatory commercial policy that indicates the type of clients the applicant firm agrees to transact with and the conditions that shall be met by these clients.
(ii) Pricing Mechanism	• The methodology for determining the price of the crypto-assets that the applicant firm proposes to exchange for funds or other crypto-assets and any applicable limit determined by the applicant firm on the amount to be exchanged. Please also outline how the volume and market volatility of crypto-assets impact the pricing mechanism.

13. Providing the Service of Executing Orders for Crypto-assets on Behalf of Clients

Where the applicant firm intends to provide the service of execution of orders for crypto-assets on behalf of clients, please provide the following information:

i. The arrangements to ensure the client has provided consent on the execution policy prior to the execution of the order;
ii. A list of the trading platforms for crypto-assets on which the applicant firm will rely for the execution of orders and the criteria for the assessment of execution venues included in the execution policy;
iii. Which trading platforms the applicant firm intends to use for each type of crypto-asset and confirmation that it will not receive any form of remuneration, discount or non-monetary benefit in return for routing orders received to a particular trading platform for crypto-assets;
iv. How the execution factors of price, costs, speed, likelihood of execution and settlement, size, nature, conditions of custody of the crypto-assets or any other relevant factors are considered as part of all necessary steps to obtain the best possible result for the client;
v. Where applicable, the arrangements for informing clients that the applicant firm will execute orders outside a trading platform and how it will obtain the prior express client consent before executing such orders;
vi. How the client is warned that any specific instructions from a client may prevent the applicant firm from taking the steps that it has designed and implemented in its execution policy to obtain the best possible result for the execution of those orders in respect of the elements covered by those instructions;
vii. The selection process for trading venues and execution strategies employed, the procedures and processes used to analyse the quality of execution obtained and how the applicant firm monitors and verifies that the best possible results were obtained for clients;

viii. The arrangements to prevent the misuse of any information relating to clients' orders by the employees of the applicant firm;
ix. The arrangements and procedures for how the applicant firm will disclose to clients information on its order execution policy and notify them of any material changes to their order execution policy; and
x. A description of the arrangements, systems and procedures to prevent and detect market abuse.

14. Providing Advice on Crypto-assets or Portfolio Management of Crypto-assets

Where the applicant firm intends to provide advice on crypto-assets or portfolio management of crypto-assets, please provide the following information:

- The policies and procedures and a detailed description of the arrangements in place to ensure that the natural persons providing advice or information possess the necessary knowledge and competence[5] to fulfil their obligations.

15. Providing Transfer Services for Crypto-assets on Behalf of Clients

Where the applicant firm intends to provide transfer services for crypto-assets on behalf of clients, please provide the following information:

i. Details on the types of crypto-assets for which the applicant firm intends to provide transfer services;
ii. A detailed description of the applicant firm's arrangements and deployed ICT and human resources to address risks promptly, efficiently and thoroughly during the provision of transfer services for crypto-assets on behalf of clients, considering potential operational failures and cybersecurity risks;
iii. A description on the rights of clients in the context of transfer services for crypto-assets and arrangements to ensure that clients are adequately informed of their rights; and
iv. A description of the applicant firm's insurance policy, if any, including on the insurance's coverage of detriment to client's crypto-assets that may result from cyber security risks.

[5] MiCAR Art 81(7) outlines "Member States shall publish the criteria to be used for assessing such knowledge and competence."

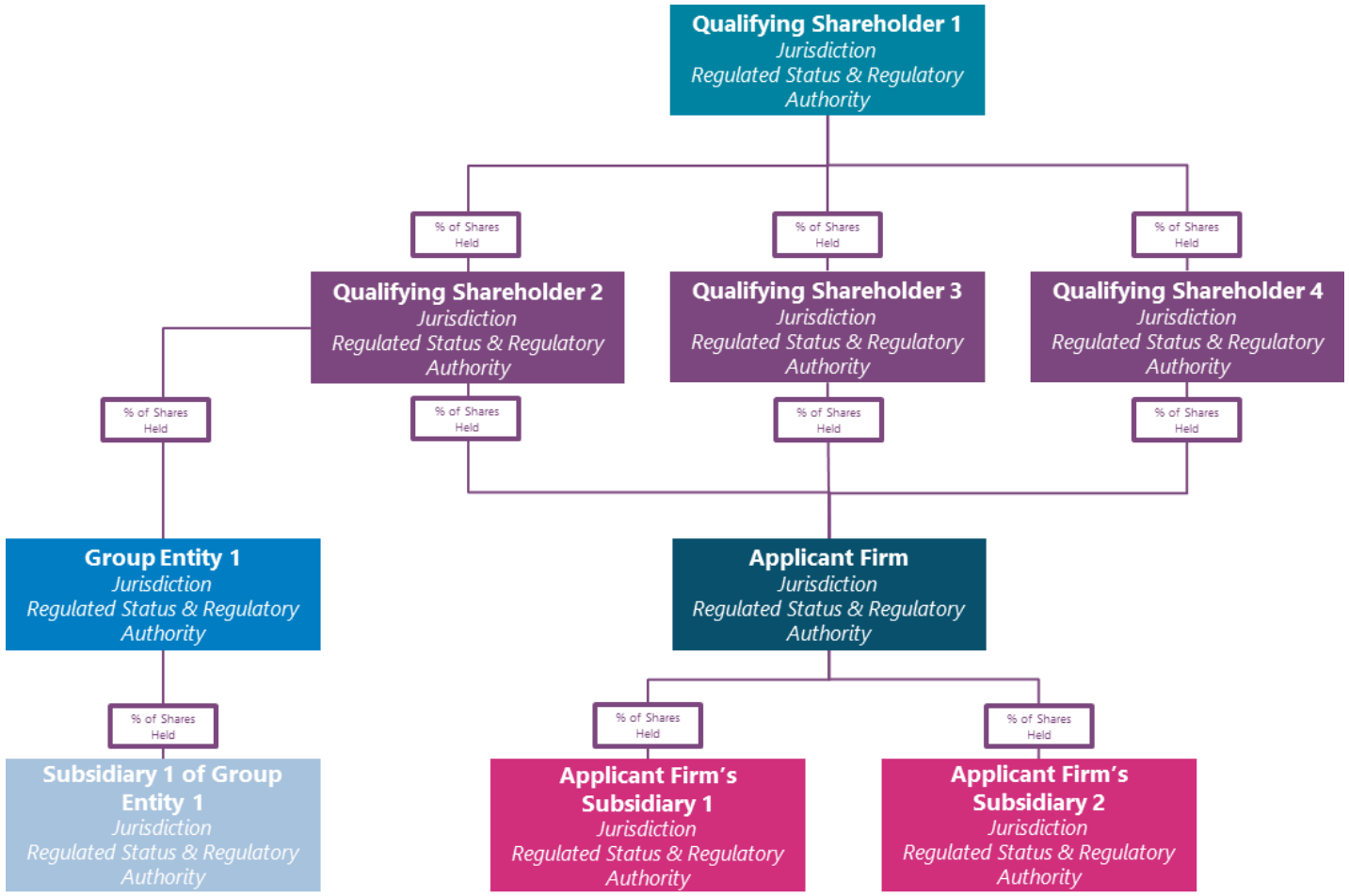
Appendix I – Outsourcing Arrangements

Please use the following table as a template provide information regarding outsourcing arrangements.

#	Outsourced Service Provider	Outsourced Service	Overview of Service Provided	Service Location	Type of Outsourcing	Critical or Important	Sub-outsourcing	No. of Available FTE	Applicant firm's Oversight Responsibility
1	*OSP #1 Name*	*Outsourced function/service name*	*High-level overview of the outsourced function/service*	*Identify the location where service is performed*	*e.g. third-party or intra-group outsourcing*	*Yes/No*	*Yes/No* *If yes, define the sub-outsourcing chain and the sub-OSP(s) location(s)*	*Number of FTE the relevant OSP has available to the applicant firm*	*Identify the individual/function responsible for outsourcing oversight*
2	*Please use separate lines for each OSP*								

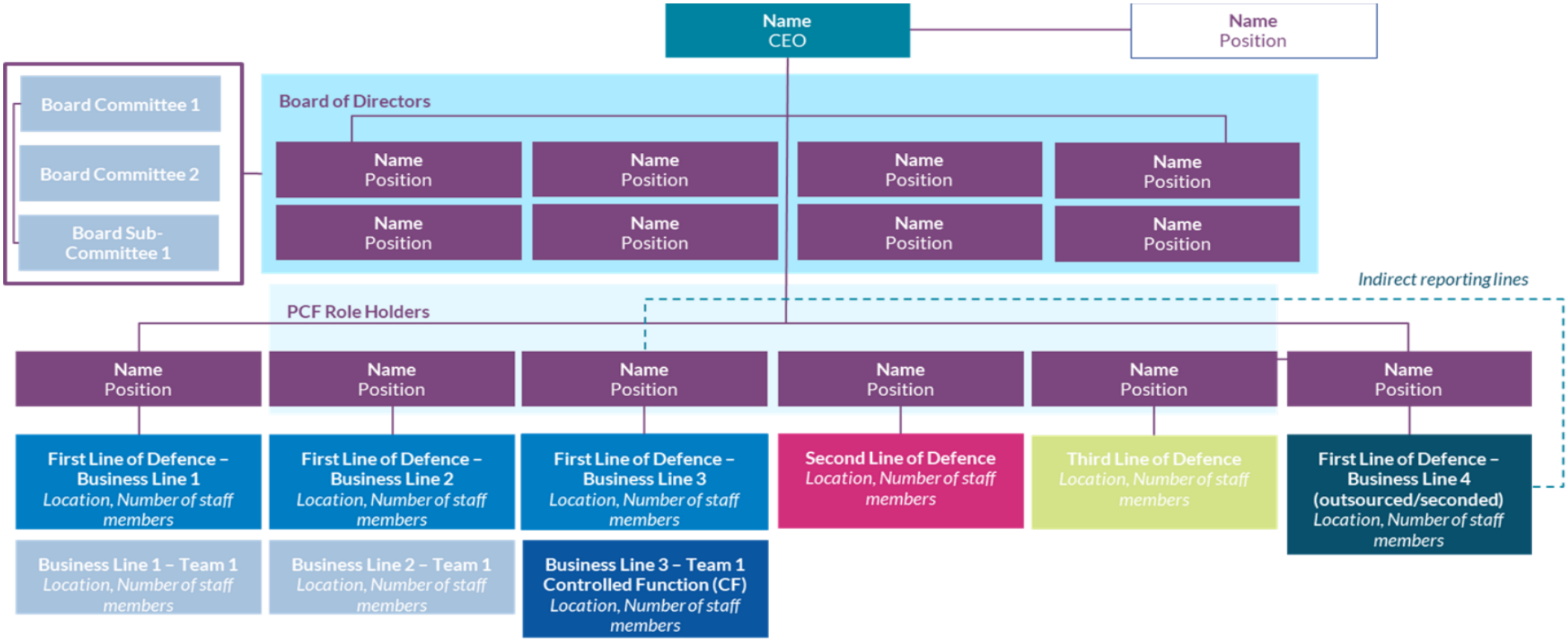
Appendix II – Ownership Structure

Please use the following indicative chart as an example provide information in relation to qualifying shareholders.



Appendix III – Organisational Structure

Please use the following indicative chart as an example to provide information in relation to organisational structure.



Appendix IV – Proposed PCFs

Please use the following table as a template to provide information regarding PCFs and board members.

Position/PCF Role	Key Roles and Responsibilities	Name of Individual	Proposed Time commitment	Residency	Previously approved by the Central Bank (Y/N)	Group Responsibilities (if any)
e.g. Independent Non-Executive Director & Chair of the Board (PCF-2, PCF-3)	*e.g. Attend and Chair Monthly Board Meetings* *-Act as an Impartial voice at Board meetings etc.*	*e.g. John Smith*	*e.g. 20 days per Annum*	*Ireland*		
e.g. Chief Executive Officer & Executive Director (PCF-8, PCF-1) etc.	*e.g. formulate strategy etc.*	*e.g. Jane Kelly*	*e.g. full time FTE*	*UK*		
Please use separate line for each position/PCF function						

Appendix V – Proposed Staffing Arrangements

Please use the following table as a template to provide information regarding staffing arrangements.

	At authorisation (Year 0)	Year 1	Year 2	Year 3	Shared[6] with other group entities (Y/N)	Employed by other group entities (Y/N/N/A)
Total proposed staff of the legal entity						*If yes, enter the entity's name and location*
of which full-time employees						*If yes, enter the entity's name and location*
of which based in Ireland						*If yes, enter the entity's name and location*
of which based in other jurisdictions						*If yes, enter the entity's name and location*
of which part-time employees						*If yes, enter the entity's name and location*
of which based in Ireland						*If yes, enter the entity's name and location*
of which based in other jurisdictions						*If yes, enter the entity's name and location*

[6] Staff members are employed by the applicant firm but are shared with other group companies.

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

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem