SEC MEMORANDUM CIRCULAR NO. 5
Series of 2025

SUBJECT: THE SEC GUIDELINES ON THE OPERATIONS OF CRYPTO-ASSET SERVICE PROVIDERS (CASP GUIDELINES)

---

1. Applicability and Scope -

1.1 These guidelines shall apply to all CASPs that are offering crypto-asset services and third-party service providers who engage in the marketing of crypto-assets and crypto-asset services.

1.2 These guidelines may be applied for the implementation of the CASP rules, the SRC or the FCPA, if appropriate.

1.3 The provisions of these guidelines are without prejudice to the issuances of other Philippine regulatory agencies in the exercise of their jurisdiction over activities related to crypto-assets.

2. ***CASP Registration*** – No CASP shall be registered unless it complies with the following:

2.1 The applicant must be a corporation registered with the SEC.

2.1.1. The operation of a CASP must be included in the primary purpose of the corporation, as indicated in its Articles of Incorporation.

2.1.2. The corporation must have a minimum paid-up capital of at least One Hundred Million Pesos (P100,000,000.00) in cash or property, excluding crypto-assets.

2.2 The applicant must have a physical office located in the Philippines which must be appropriately staffed or manned during regular business hours, in compliance with the relevant provisions of the Revised Corporation Code and other issuances by the SEC, as applicable.

2.3 The applicant shall submit CASP Form 1 (Annex 1), together with the following certified documents to the PhiliFintech Innovation Office (PhiliFINNO) at fintech@sec.gov.ph :

2.3.1. Listing and delisting standards for admission of crypto-assets to trading, as described in paragraph 5.3 of these guidelines;

2.3.2. Trading and disclosure rules;

2.3.3. Business conduct rules;

2.3.4. A continuing authorization for the Commission's duly authorized representative to verify the applicant's bank accounts;

2.3.5. A written description of the software system or program which shall include a flowchart showing a market transaction, and a diagram or matrix showing its applications and functions;

2.3.6. A written description of software and hardware components, as well as the communication facility of the system, which shall include configuration, capacity,

Published:
Philippine Daily Inquirer, 4 June 2025
Philippine Star, 4 June 2025

Filed with UP Law Center: 2 June 2025

interconnection with other CASP or other trading markets, and extent of communication ability;

2.3.7. Description of the custodian or registrar of the crypto-assets to be traded in the system and the related systems to be used;

2.3.8. Copy of the Board Resolution approving and authorizing the company's registration as a CASP;

2.3.9. Curriculum vitae of all the management and information technology personnel in charge or directly responsible for the system;

2.3.10. Copy of any agreement executed or license granted pertaining to the operation of the system and to the product/s proposed to be offered. The copy of all other contracts, Memorandums of Understanding entered into with any party by the CASP, and any amendment shall be submitted to the Commission for approval;

2.3.11. A risk disclosure matrix discussing the risk factors involved in the operation of the platform, which includes the following:

2.3.11.1. Process of identification of risks;

2.3.11.2. Description of the risks involved;

2.3.11.3. Assessment and valuing of risks; and

2.3.11.4. Risk management.

2.3.12. A description of an independent risk control unit that will be responsible for the design and implementation of the company's risk management system;

2.3.13. Business plan which shall include, but not limited to, any and all trade names, digital or other platforms to be used, marketing strategies, and financial plan for the next twelve months or such longer period as the Commission may prescribe;

2.3.14. An undertaking that the board of directors and senior management shall be actively involved in the risk control process and must regard the control as an essential aspect of the business to which significant resources must be devoted; and

2.3.15. Proof of payment of filing fees.

2.4 The applicant shall show proof that the corporation has met the minimum capital requirement under these guidelines and that the corporation has sufficient financial resources, not including crypto-assets, to ensure that the business is resilient, including the ability to meet all debts as they fall due, and adequate provision for any contingent and foreseeable liabilities.

2.5 The applicant shall submit the procedure for the clearing/settlement of the trades undertaken under the CASP, including an undertaking that all obligations arising from such trading shall be met.

2.6 The Commission may impose other requirements and/or conditions for the registration of the CASP, as may be deemed necessary to protect the investing public.

3. Exemption from Registration -

3.1 The Commission, by an order, after an application for exemption from CASP registration has been filed, may grant such exemption after determining that said order is consistent with the public interest and the protection of investors.

4. Admission to Trading of Crypto-Assets –

4.1 A CASP shall comply with Section 5 of the CASP Rules in offering a crypto-asset in the Philippines.

4.2 The CASP shall ensure that all available information from reputable or credible sources pertaining to the product/s being traded in the system is provided to the investors.

4.3 CASPs must maintain and implement clear and objective listing and delisting standards regarding crypto-assets and must apply those standards when considering the admission to trading, suspension, or delisting of crypto-assets.

4.3.1. Listing rules must be disclosed to the SEC and accessible in a clear place on the CASP's main website.

4.3.2. Before admitting any crypto-asset to trading, the CASP must assess the suitability of the crypto-asset for listing in accordance with the CASP's listing and operating rules, and the requirements of the CASP Rules and Guidelines. The assessment must include as a minimum:

4.3.2.1. The technical security and reliability of the crypto-asset;

4.3.2.2. Any association of the crypto-asset to illegal or fraudulent activities;

4.3.2.3. The experience, track record, and reputation of the crypto-asset issuer or any associated foundation or protocol; and

4.3.2.4. Whether the crypto-asset project was offered through a fundraising activity or has the features of a crypto-asset security.

4.4 The SEC shall have the power to order the removal or suspension of a crypto-asset in a CASP, in the interest of investor protection.

4.5 Crypto-assets services may not involve crypto-assets having features that are prohibited as prescribed by the Commission including, but not limited to, those related to gambling activities and obfuscation of identity and/or transactions.

4.6 Unless allowed by the Commission, CASPs should not conduct any offering, trading, or dealing of derivatives involving crypto-assets, as well as offer trading on leverage.

*5. **Operational Requirements*** - During the effectivity of the registration as a CASP, the following requirements shall be complied with:

5.1 Business conduct - CASPs must at all times act honestly, fairly, and professionally in accordance with the best interests of their clients and prospective clients.

5.2 Fair access – a CASP shall:

5.2.1. Establish written standards for granting or denying access to trading on its platform, including its monitoring and recordkeeping;

5.2.2. Not unreasonably prohibit or limit any person in respect to access to services offered by such CASP by applying the standards in an unfair or discriminatory manner; and

5.2.3. Report the information required regarding grants, denials, and limitations of

access.

5.3 Capacity, integrity, and security of automated systems - With respect to systems that support order entry, order routing, order execution, transaction reporting, and trade comparison, the CASP shall:

5.3.1. Establish a local data center in order to make clear the jurisdictional and regulatory control of the SEC over the CASP, its operations, and its personnel. Should the CASP opt to outsource critical IT systems to service providers outside the Philippines, it shall be subject to the following conditions:

5.3.1.1. Explain why the outsourced system is essential to their operations and the reason why it cannot be done locally.

5.3.1.2. The CASP shall adopt additional measures to address risks involved in the outsourcing arrangement.

5.3.1.3. The CASP shall be responsible for the performance of the service in the same manner and to the same extent as if it were directly performing the said activity.

5.3.2. Establish reasonable current and future capacity estimates;

5.3.3. Develop and implement reasonable procedures to review and keep current its system development and testing methodology;

5.3.4. Review the vulnerability of its systems and data center computer operations to internal and external threats, physical hazards, and natural disasters;

5.3.5. Establish adequate contingency, disaster recovery, and backup disaster recovery plans;

5.3.6. On an annual basis, allow an independent review, in accordance with established audit procedures and standards, of such CASP's controls to ensure that the requirements in this section are met. The report of which, including its recommendations and conclusions, shall be reviewed and implemented by senior management when appropriate.

5.4 Risk Mitigation - CASPs must have appropriate risk management frameworks (including people, processes, systems and controls) in place to manage and mitigate such risks. CASPs must put in place sufficient measures to address cyber and system resiliency. These measures should be reviewed at least annually and updated to help ensure that they remain strong and robust. Such measures could include:

5.4.1. identifying the relevant operational and technological risks which the CASP faces and requiring the CASP to adopt appropriate processes and procedures to address such risks.

5.4.2. implementing operational and technology risk management framework and conducting at least an annual independent audit from a reputable third party.

5.4.3. implementing frequent, rigorous code audits to mitigate cyber security risks.

5.5 Client Contact - CASPs must have an effective procedure allowing clients to get in touch easily for support, which provides clients with a prompt response to any queries. Clients must be able to contact the CASP by a suitable written digital communication method.

5.6 Complaints handling - CASPs must maintain an effective and free-of-charge

complaints procedure and must make details of how to access this procedure readily and easily available to clients. Clients must be notified about the complaints procedure and CASPs must ensure that queries receive a prompt and fair response.

5.7 Market monitoring – CASPs must establish and maintain effective arrangements, systems and procedures aimed at preventing, detecting, and taking action in respect of market abuse, insider dealing, unlawful disclosure of inside information and market manipulation, cyber risks, and other financial crimes.

5.7.1. CASPs should ensure that any systems allow them to effect timely surveillance of transactions and orders and allow the CASP to take prompt action following discovery of relevant practices, including where appropriate suspension of trading. Conduct periodic capacity stress tests of critical systems to determine the system's ability to process transactions in an accurate, timely, and efficient manner;

5.8 Limited offering - The CASP shall be limited to the activities described in its certificate of registration unless a request for inclusion of changes thereto is filed to and approved by the Commission.

5.9 Examinations, inspections, and investigations - The CASP shall permit the examination and inspection of its premises, systems, and records, and cooperate with the examination, inspection, or investigation of subscribers, whether such examination is conducted by the Commission or by another regulatory agency.

5.10 Orderly wind-down - CASPs are required to have plans to ensure an orderly cessation of their activities, whilst ensuring an appropriate level of protection for clients and client assets. CASPs must provide details of wind-down plans to the SEC promptly on request.

6. Segregation and Safeguarding of Customer Assets - All crypto-assets that CASPs hold in custody must be legally and operationally segregated from the CASP's own assets in accordance with applicable law and so that such assets are not available to other creditors of the CASP in the event of insolvency.

6.1 A CASP which provides custody activities must implement robust measures and safeguards to protect client crypto-assets and any means of access to such crypto-assets and must take adequate steps to minimize the risk of loss of client assets.

6.2 CASPs that provide custody services must not use client crypto-assets for their own account and must put in place adequate measures to prevent such usage. Any crypto-assets held must always be legally unencumbered.

6.3 CASPs shall not engage in proprietary trading using customer funds unless with the consent of the customer was previously acquired, and approved by the SEC.

7. Client Suitability -

7.1 CASPs shall establish procedures to ensure that their clients understand the risks associated with investing in crypto-assets and are financially able to satisfy any obligation that may arise from purchasing the financial product. The CASP must

consider the following in its assessment:

7.1.1. Knowledge and experience in investing in crypto-assets;

7.1.2. Investment objectives including, but not limited to, risk tolerance, time horizon, and venues through which they can acquire crypto-assets;

7.1.3. Financial circumstances including, but not limited to, their ability to bear sudden and significant losses or the proportion of their net worth that is invested in crypto-assets; and

7.1.4. A determination of whether or not the amount and terms of the offered product or service allow clients to meet their respective obligations with a low probability of serious hardship, and that there is a reasonable prospect that the product or service will provide value to its client.

7.2 Should the CASP find a person not suitable to participate in the offered products or services, such person should not be allowed to use the platform.

8. Anti-Money Laundering and Countering Terrorism Financing **-** CASPs must adhere to any legal requirements with respect to anti-money laundering and countering terrorism financing requirements, as provided in the CASP Rules, SEC issuances, and other relevant laws and regulations.

9. Cybersecurity **-** CASPs must ensure there are robust security policies, processes and controls in place in accordance with best industry practice and international standards, including:

- Secure authentication and client identification methods;
- Use of data encryption and secure transfer technology;
- Implementation of monitoring and alerting systems to detect risks, critical issues, and incidents;
- Maintenance logs of data access, particularly with respect to sensitive data;
- Maintenance logs and audit trails in respect of critical events, including system changes, access attempts, and configuration changes; and
- Staff training.

9.1 CASPs must regularly audit, monitor, and update any security controls, both periodically and following any material cybersecurity event, and must maintain records of audits completed and actions required. CASPs must complete a periodic independent assessment of cybersecurity at least annually, which must consider the security features of all technical systems relevant to the CASP's services, including wallets, user applications, network and system security, and physical security factors.

10. Outsourcing -

10.1 CASPs shall not outsource any services or activities to third parties if this would materially affect or impair:

10.1.1. The CASP's exposure to operational risks;

10.1.2. The quality of the crypto-asset service provider's internal controls; or

10.1.3. The ability of the SEC and other competent authorities to exercise their statutory rights or to monitor, supervise or audit the crypto-asset service provider's compliance with all applicable laws or regulatory requirements.

10.2 CASPs remain responsible at all times for their regulated services and may not delegate responsibility to third parties. CASPs are responsible for the activities, actions, and omissions of any third-party outsourcing entity in respect of regulated services.

10.3 All outsourcing arrangements must be documented in written agreements and CASPs must ensure that the CASP has the right to terminate such agreements on a reasonable period of notice. CASPs must maintain a written policy on outsourcing, including an assessment of outsourcing risks and their risk management strategy, including approach to exiting outsourcing arrangements and taking into account the extent and type of outsourcing and the services affected, as well as ensuring adequate protection for the interests of clients of the CASP, protection of their personal data and management of technical and operational risks.

10.4 CASPs must comply with all guidance and principles issued by the SEC and applicable to material outsourcing arrangements. In particular, CASPs must ensure that, where a CASP subcontracts any licensed activities, there is a written agreement in place requiring that the third party must provide equivalent standards and be accountable to the SEC, including providing any access to information or premises required for the SEC to perform checks and audits.

10.5 CASPs shall adopt a sound risk management system to mitigate risks arising from outsourcing (i.e. confidentiality of information, data privacy, data management, contract management, security, performance monitoring and business continuity, among others). The CASP shall be responsible for the performance of the service in the same manner and to the same extent as if it were directly performing the relevant activity.

11. Grounds for Suspension or Revocation -

11.1 The SEC may refuse, withdraw, terminate, suspend, or revoke the authorization of any crypto-asset services in cases when the CASP:

11.1.1. Fails to meet the requirements of the CASP Rules and Guidelines, or in the exercise of the SEC's sound discretion, is reasonably determined to be unable to meet the requirements of the CASP Rules and Guidelines in the future;

11.1.2. Has not used its authorization within twelve (12) months from the date of its grant;

11.1.3. Ceases to operate or to provide crypto-asset services;

11.1.4. Breaches any requirement of the CASP Rules or Guidelines, or whose Certificate of Authority granted under the CASP Rules has been withdrawn, expired, or revoked;

11.1.5. Fails to take action to remedy a breach of CASP Rules or Guidelines within the timeframe required by the SEC;

11.1.6. Has violated any of the provisions of the CASP Rules, CASP Guidelines, or any order of, or relevant laws or regulations issued by, the

Commission; or

11.1.7. Has made any false or misleading representation of material facts in any disclosure document, communication, reports, or any other document, or has submitted an application for registration or authorization that is on its face incomplete or inaccurate in any material respect, or includes any untrue statements of a material fact required to be stated therein or necessary to make the statement therein not misleading, or the information contained in the application for registration or authorization, disclosure document, communication, reports, or any other document submitted by the crypto-assets service provider has become misleading, incorrect, inaccurate, inadequate or incomplete in any material respect;

11.1.8. Has been or is engaged or is about to engage in fraudulent sale, marketing, distribution or transaction of crypto-assets;

11.1.9. Has been given an audit opinion, other than unmodified or unqualified, by an independent auditor considering the facts and circumstances surrounding its findings. This is without prejudice to the sanctions as provided by the Revised Corporation Code and other relevant laws.

11.1.10. Has committed any acts in violation of, or considered as violations in, or has been a subject of any order, decision, or circumstance warranting the suspension or revocation of authorization as provided by the SRC, the FCPA or other relevant laws or regulations enforced by the SEC; or

11.1.11. Expressly terminates or renounces its authorization.

11.2 Notwithstanding the foregoing, nothing in these Guidelines shall be construed as limiting the SEC's authority, and for purposes of investor protection, withdraw, terminate, or suspend a CASP license and take any other appropriate action as the SEC may deem fit.

12. Suspension or Revocation of CASP License -

12.1 The Commission may require from the CASP such further information as may in its judgment be necessary to enable the Commission to ascertain whether the registration of such CASP should be revoked on any ground specified under the CASP Rules or Guidelines. The Commission may also suspend the privilege to operate the CASP, including the trading of crypto-assets, pending further investigation, by issuing an order specifying the grounds for such action.

12.2 Upon issuance of an order of suspension, the Commission within five (5) days shall conduct a hearing. Thereafter, if the Commission determines that the registration should be revoked, it shall issue an order revoking the same.

12.3 Pending the issuance of a final order, the suspension of a CASP shall be deemed confidential, and shall not be published, unless it shall appear that the order of suspension has been violated after notice. If, however, the Commission finds no basis for such suspension, it shall forthwith issue an order lifting the order of suspension.

12.4 In the interest of the public and for the protection of investors, the Commission, whenever it has reason to believe so, may direct a CASP to take such action as it considers necessary to maintain or restore orderly trading in, or liquidation of, any

contract including but not limited to:

12.4.1. Terminating or suspending trading on a CASP;
12.4.2. Confining trading to the liquidation of contracts;
12.4.3. Ordering the liquidation of all positions or part thereof or the reduction in such positions;
12.4.4. Limiting trading to a specific price range;
12.4.5. Fixing or modifying trading days or hours;
12.4.6. Fixing the settlement price at which contracts are to be liquidated;
12.4.7. Requiring any person to act in a specified manner in relation to trading in the CASP;
12.4.8. Requiring additional margins for any contracts; and
12.4.9. Modifying or suspending any of the business rules of the CASP.

13. Prohibited Acts – No person or entity shall engage in the following:

13.1 To act as a CASP without being duly authorized by the Commission.

13.2 To establish any office or place of business anywhere in the Philippines for the purpose of engaging in crypto-asset services unless registered with the Commission.

13.3 To represent himself falsely to be a subscriber, operator or provider of a CASP, or an affiliate thereof in soliciting or handling any transaction, or to represent falsely in connection with any transaction.

14. Fraud, Manipulation and Insider Trading -

14.1 No person shall engage in the prohibited acts and practices provided in Chapter VII of the Securities Regulation Code and relevant provisions of the Implementing Rules and Regulations of the said Code, in relation to the trading of crypto-assets.

15. Reportorial Requirements and Record-Keeping -

15.1 A CASP shall maintain an operational report and make it available to the SEC for examination, that as a minimum should contain the following:

15.1.1. Record of users:
15.1.1.1. Total Number
15.1.1.2. Active users
15.1.2. Daily trading summaries:
15.1.2.1. Number of trades
15.1.2.2. Number of crypto-assets traded
15.1.2.3. Total settlement value
15.1.2.4. Time-sequenced records of order information:
15.1.2.5. Date and time (expressed in terms of hours, minutes, and seconds) the order was received;
15.1.2.6. Crypto-asset identifier;
15.1.2.7. The number of crypto-assets or contracts to which the order applies;
15.1.2.8. The designation of the order as a buy or sell order;

15.1.2.9. If a sell order, the designation as a sell long or a sell short order.
15.1.2.10. The designation of the order as a short sale order;
15.1.2.11. The designation of the order as a market order, limit order, or other type of order;
15.1.2.12. The limit or stop price prescribed by the order;
15.1.2.13. The date on which the order expires and, if the time in force is less than one (1) day, the time when the order expires;
15.1.2.14. The time limit during which the order is in force;
15.1.2.15. Any instruction to modify or cancel the order;
15.1.2.16. The type of account, i.e., retail, wholesale, affiliate, proprietary, or any other type of account designated by the CASP, for which the order is submitted;
15.1.2.17. Date and time (expressed in terms of hours, minutes, and seconds) that the order was executed;
15.1.2.18. Price at which the order was executed;
15.1.2.19. Size of the order executed (expressed in number of shares or units or principal amount); and
15.1.2.20. Identity of the parties to the transaction.

15.2 On a monthly basis, CASPs shall as a minimum submit to the SEC the following information:

15.2.1. Statement of financial position;
15.2.2. Statement of profit and loss and other comprehensive income;
15.2.3. Statement of cash flows;
15.2.4. List of off-balance sheet items, if any;
15.2.5. Addresses of their crypto-asset wallets;
15.2.6. A full list of entities in their group that actively invest their own, or the group's portfolio in crypto-assets, and a complete record of all transactions, including but not limited to loans or any transactions involving any crypto-asset activity for which the CASP is authorized, with all such persons or entities identified; and
15.2.7. Transactions with related parties.

15.3 On a quarterly basis, CASPs shall as a minimum submit to the SEC the following information:

15.3.1. The minutes of all Board meetings and Board committee meetings;
15.3.2. A statement demonstrating compliance with any financial requirements established by the SEC;
15.3.3. Financial projections and strategic business plans; and
15.3.4. A risk exposure report prepared and submitted to the Board.

15.4 On an annual basis, CASPs shall as a minimum submit to the SEC the following information:

15.4.1. Audited annual financial statements, together with an opinion and an attestation by an independent third-party auditor regarding the effectiveness of the

CASP's internal control structure;

15.4.2. An assessment by Senior Management of the CASP's compliance with such applicable laws, regulations, rules and issuances during the fiscal year covered by the financial statements;

15.4.3. Certification of the financial statements by a member of the Board or a Responsible Individual attesting to the truth and correctness of those statements;

15.4.4. A representative sample of all documentation relating to client onboarding, including actual documentation of the first one hundred [100] clients onboarded of the year;

15.4.5. Descriptions of product offerings relating to their crypto-asset activities; and

15.4.6. General information sheet.

15.5 A CASP shall preserve the following records for at least five (5) years:

15.5.1. All notices provided by such CASP to users generally, whether written or communicated through automated means, including, but not limited to, notices addressing hours of system operations, system malfunctions, changes to system procedures, maintenance of hardware and software, instructions pertaining to access to market and denials of, or limitations on, access to the CASP;

15.5.2. All documents relevant to the CASP decision to grant, deny, or limit access to any person, and all other documents made or received by the CASP in the course of complying with fair access; and

15.5.3. At least one copy of all documents made or received by the CASP in the course of complying with system resilience standards, including all correspondence, memoranda, papers, books, notices, accounts, reports, test scripts, test results, and other similar records.

15.6 The SEC may require upon request to a CASP, information to be provided in addition to those listed in this section.

16. Fees and Penalties -

16.1 Registration fee – All applications for registration shall be accompanied by an initial filing fee of Fifty Thousand Pesos (P50,000.00) or such amount as the Commission may determine.

16.2 Supervision fee – CASPs shall pay to the Commission, on a semestral basis on or before the tenth (10th) day of the end of every semester of the calendar year, a supervision fee based on the gross revenue of such CASP during the preceding year for the privilege of doing business, during the preceding calendar year or any part thereof. It shall be computed as follows:

First Two Billion Pesos (P2,000,000,000.00) of gross revenue	1/300 of 1%
For the next Two Billion Pesos	1/200 of 1%

(P2,000,000,000.00) of gross revenue	
Onwards	1/100 of 1%

16.3 Penalty for late or non-filing of reports – Ten Thousand pesos (P10,000.00) basic fine, plus Five Hundred pesos (P500.00) per day of delay.

16.4 Penalty for any violation of these Guidelines –

First instance	Fifty Thousand Pesos (P50,000.00) per violation
Second instance	One Hundred Thousand Pesos (P100,000.00) per violation
Third instance and onwards	Two Hundred Thousand Pesos (P200,000.00) per violation, and cancellation of registration

17. The PhiliFINNO, or such other unit as the Commission may create, shall be the primary body in the implementation of the CASP Rules and the CASP Guidelines and the supervision of CASPs, among other relevant departments of the Commission.

18. ***Separability Clause*** **-** If any portion or provision of these Guidelines is held unconstitutional or invalid, all other provisions not thereby affected shall remain valid.

19. ***Repealing Clause*** - All other rules and regulations or parts thereof, inconsistent with the foregoing rules and regulations, are repealed, amended, or modified accordingly.

20. ***Effectivity Clause*** **-** This Circular shall take effect within thirty (30) days after the completion of its publication in two (2) newspapers of general circulation.

Makati City, Philippines, 30 May 2025.

For the Commission:

EMILIO B. AQUINO
Chairperson

ANNEX 1

CASP Form 1

CASP APPLICATION FORM

GENERAL INSTRUCTIONS

1. The CASP Form 1 shall be used for the application for the CASP License under the SEC Crypto Assets Service Providers Guidelines.
2. This application form shall be signed by the principal executive officer, president, or persons performing similar functions in the corporation.
3. Any information required in the CASP Form may be incorporated by indicating the annex number in which the information may be found. The authorized officer of the applicant should sign each attachment.

Name of the applicant:	
SEC Registration No.:	
Address:	
Contact details, as registered according to MC 28-2020:	
Trade name, website, or application to be used:	

Contact Person

Name:	
Designation in the Corporation:	
Contact No.:	
Email:	

I. Governance

List of directors and officers of the corporation including their age, nationality, addresses, and their profile.	
A detailed description of the organizational structure of the applicant, including the distribution of tasks and powers, relevant reporting lines, and internal control arrangements, together with an organizational chart.	
The personal details of the heads of internal functions (management, supervisory, and internal control functions), including their residence and a curriculum vitae. It should include relevant education, professional training, and professional experience, as well as a description of the skills, knowledge, and expertise required to discharge the responsibilities allocated to them.	
The policies and procedures, along with a detailed description of the arrangements in place to ensure that relevant staff are aware of the policies and procedures that must be followed to properly discharge their responsibilities.	
The policies and procedures and a detailed description of the arrangements put in place to maintain adequate and orderly records of the business and internal organization of the applicant.	
The policies and procedures and arrangements to enable the management body to assess and periodically review the effectiveness of the policy arrangements and procedures put in place.	
A description of the arrangements put in place to prevent and detect market abuse and fraudulent activities.	
A description of the company's policies on conflicts of interests.	

II. Operations

Technical documentation of the ICT systems, including the DLT infrastructure relied upon, where relevant, and the security arrangements.	
Description and location of the data center.	
A business plan which shall include: • Marketing strategies; and • Financial plan for the next 12 months.	
Trading and disclosure rules.	
Business conduct rules.	
List of bank accounts, with a continuing authorization for the Commission's duly authorized representative to verify.	
Description of any relevant agreements or licenses concerning the operation of the platform or the service or products to be offered.	
Risk disclosure matrix including: • Process of identification of risks; • Description of the risks involved; • Assessment and valuing of risks; and • Risk management.	
Description of the independent risk control unit.	
Detailed description of the procedures governing the execution, reporting, clearance, and settlement of transactions or trades.	
Any exchange of crypto-assets for funds and other crypto-asset activities that the applicant intends to undertake, including through any decentralised finance applications with which the applicant wishes to interact on its own account.	
Current and future capacity estimates, contingency, and business continuity plans. Procedures for the review of system capacity, security, and contingency planning procedures.	

III. Products and Investors

A list of crypto-asset services that the applicant intends to provide as well as the types of crypto-assets to which the crypto-asset services will relate.	
Rules regarding the admission of crypto-assets to trading, including its approval process.	
The policies and procedures adopted to assess the suitability of crypto-assets.	
Target customer demographics.	
Screening mechanism and criteria for qualification for customer onboarding.	
A description of all fees to be paid by customers, including fees relating to connection to the system, access, data, regulation (if applicable) and how such fees are set.	
Description of mechanisms to ensure that the clients understand the risks associated with investing in crypto-assets and crypto-asset services, and are financially able to satisfy any obligation that may arise.	
A description of the means of access to the applicant's crypto-asset services by clients, including the domain names for each website or other ICT-based application through which the applicant will provide the crypto-asset services and the types of crypto-asset services that will be available.	

IV. Affiliates and Third-party service providers

List of affiliates and third-party service providers.	
An explanation of how the activities of the entities affiliated with the applicant, including where there are regulated entities in the group, are expected to impact the activities of the applicant. This explanation shall include a list of and information on the entities affiliated with	

the applicant, including those that are regulated entities. It shall also provide details on the services provided by these entities (including regulated services, activities, and types of clients) and the domain names of each website operated by such entities.	
The applicant's outsourcing policy and a detailed description of the applicant's planned outsourcing arrangements. The applicant shall also include information on the functions or person responsible for outsourcing, the resources (human and ICT) allocated to the control of the outsourced functions, services or activities of the related arrangements and on the risk assessment related to the outsourcing.	

V. Anti-Money Laundering Measures

The applicant's assessment of the inherent and residual risks of money laundering and terrorist financing associated with its business, including the risks relating to the applicant's customer base, the services provided, and the distribution channels used.	
The measures that the applicant has or will put in place to prevent the identified risks and comply with applicable anti-money laundering and counter-terrorist financing requirements, including the applicant's risk assessment process, the policies and procedures to comply with customer due diligence requirements, and the policies and procedures to detect and report suspicious transactions or activities.	
The identity of the person in charge of ensuring the applicant's compliance with anti-money laundering and counter-terrorist financing obligations, and evidence of the person's skills and expertise.	

A copy of the applicant's anti-money laundering and counter-terrorism policies procedures, and systems.	
The frequency of the assessment of the adequacy and effectiveness of such mechanisms, systems, policies and procedures, as well as the person or function responsible for such assessment.	

VI. Segregation of Customer Funds

How the applicant ensures that: • Client's funds are not used for its own account; • Crypto-assets belonging to the clients are not used for its own account; • The wallet holding the client's crypto-assets is different from the applicant's own wallets.	
A detailed description of the approval system for cryptographic keys and safeguarding of cryptographic keys (for instance, multi-signature wallets)	
How the applicant segregates clients' crypto-assets, including from other clients' crypto-assets, in the event of wallets containing crypto-assets of more than one client (omnibus accounts).	