Consultation Paper

AFSA-L-CE-2023-0002

Proposed Astana International Financial Centre Digital Asset Service Providers Framework

Unrestricted

2 June 2023

Introduction

Why are we issuing this Consultation Paper (CP)?

1. The Astana Financial Services Authority (AFSA) has issued this Consultation Paper to seek suggestions from the market on the amendments to the AIFC Rules and regulations to enhance the AIFC Digital Asset Trading Facility Framework.

Who should read this CP?

2. The proposals in this paper will be of interest to current and potential AIFC participants dealing with digital assets as well as the market and other stakeholders.

Terminology

3. Defined terms have the initial letter of the word capitalised, or of each word in a phrase. Definitions are set out in the Glossary Rules (GLO). Unless the context otherwise requires, where capitalisation of the initial letter is not used, the expression has its natural meaning.

What are the next steps?

4. We invite comments from interested stakeholders on the proposed framework. All comments should be in writing and sent to the address or email specified below. If sending your comments by email, please use "Consultation Paper AFSA-L-CE-2023-0002" in the subject line. You may, if relevant, identify the organisation you represent when providing your comments. The AFSA reserves the right to publish, including on its website, any comments you provide, unless you expressly request otherwise. Comments supported by reasoning and evidence will be given more weight by the AFSA.

5. The deadline for providing comments on the proposed framework is 2 **July 2023**. Once we receive your comments, we shall consider if any refinements are required to this proposal.

6. AFSA prefers to receive comments by email at consultation@afsa.kz or posted to:
   Policy and Strategy Division
   Astana Financial Services Authority (AFSA)
   55/17 Mangilik El, building C3.2, Astana, Kazakhstan

Structure of this CP

Part I – Background;
Part II – Issues;
Part III – Best Practice;
Part IV – Proposals;
Part V – Public Consultation Questions;
Part VI – Outcomes.
Annex 1 - Draft AIFC Rules on Digital Asset Activities (Digital Asset Service Providers framework);
Annex 2 – Consequential amendments to AIFC Regulations and Rules.

Background

Digital Asset Service Providers (the “DASPs”) are companies or entities that offer digital asset-related services such as exchanges, wallet providers, custody, and transfer services.

A total global market cap of digital assets amounts to $1.24 trillion as of April 2023[1]. The global DASP market is expected to witness significant growth in the coming years due to the increasing adoption of blockchain technology and virtual assets. The increasing demand for cryptocurrencies, digital securities, and other virtual assets is driving the growth of the DASP market.

However, the DASP market faces several challenges, such as regulatory uncertainty, cybersecurity risks, and money laundering concerns. Regulators across the world are introducing new laws and regulations to address these challenges and ensure the safe and secure operation of DASPs.

Regulating Digital Assets Service Providers is challenging and requires a comprehensive regulatory regime consisting of relevant licensing and regulatory requirements for DASPs' operations.

Development of the AIFC Digital Asset Service Providers Framework (the “DASPs Framework”) was prompted by the need to introduce appropriate regulatory regime for persons wishing to provide financial services activities in respect of digital assets.

The DASPs Framework aimed to:

- introduce relevant investor protection requirements in this area, while also facilitating the development of this market in a responsible and prudent manner. Proper regulation can help ensure the security and stability of the digital asset markets, reduce volatility, and provide greater confidence to participants;
- help combat illicit activities such as money laundering and terrorist financing, which are often facilitated through the use of digital assets, and provide the greater transparency and accountability;
- help facilitate the growth and adoption of digital assets as a legitimate means of exchanging value. By establishing clear rules for digital asset service providers, this Framework can provide clarity and certainty to businesses and investors, encouraging innovation and growth in the industry.

As of April 2023, Fintech Lab (Sandbox) has 10 Digital Asset Service Providers carrying on the following Regulated Activities:

- Providing Custody
- Operating a Digital Asset Trading Facility
- Arranging Custody
- Dealing in Investments as Principal
- Dealing in Investments as Agent
- Managing Investments
- Advising on Investments, Arranging Deals in Investments
- Operating an Exchange
- Operating a Clearing House
- Providing Money Services
- Arranging Deals in Investments.

[1] https://coinmarketcap.com/

Issues

The absence of a clear legal and regulatory framework for digital assets can lead to a lack of investors' confidence in those assets. Besides, it may also lead to missed opportunities in terms of innovative digital services and new funding sources for AIFC Participants.

The lack of a framework on digital assets can also hinder digital asset service providers to scale up their business. Despite the fact that the digital asset market is still modest in size, it may pose a significant a threat to the AIFC financial stability in future. Therefore, the AFSA developed a framework which will regulate activities of the VASPs.

Best Practice

We took into consideration the directions given by international standard-setters, including the Financial Action Task Force (FATF), Financial Stability Board (FSB) and the International Organization of Securities Commissions (IOSCO) in respect of Digital Assets.

The regulatory developments in other jurisdictions, including the DIFC, ADGM, UK and Bahrain, were analyzed.

Primarily, the legal framework of the DIFC is selected as a benchmark due to similar status of international financial centre with risk-based regulation and comprehensive regulatory framework for DASPs embracing many aspects of their activities.

Dubai International Financial Centre ("DIFC")

In March 2021, the DFSA introduced the Investment Token Framework with the intention of:

a) Clarifying the application of the financial services regime to persons undertaking activities that involve, or relate to, Investment Tokens; and

b) Putting in place a consistent, risk based and proportionate application of financial regulation to products, services and activities involving Investment Tokens.

In March 2022 the Crypto Token Framework was introduced, describing a regulatory regime for persons wishing to provide financial services activities in respect of Crypto Tokens. It requires all entities intending to offer financial services in relation to Crypto Tokens to establish in the DIFC as a Body Corporate and be incorporated under DIFC Law.

The Crypto Token Regime has:

- extended the scope of many existing financial services activities including advising, dealing, arranging, trading and custody, to apply to the provision of products and services in relation to Crypto Tokens;
- implemented a wide range of amendments to existing laws and rulebook modules in the DIFC; and
- limited the use of Crypto Tokens to be those which are "recognised" by the DFSA.

The following Financial Services activities are allowed for the provision of services in relation to Crypto Tokens:

a)Dealing in Investments as Principal;

b) Dealing in Investments as Agent;

c) Arranging Deals in Investments;

d) Managing Assets;

e) Advising on Financial Products;

f) Operating an Exchange;

g) Providing Custody;
h) Arranging Custody;
i) Operating a Clearing House; and
j) Operating an Alternative Trading System.

Abu-Dhabi Global Market ("ADGM")

The ADGM's Virtual Asset framework has been designed for Multilateral Trading Facilities using virtual assets, custodians and other intermediaries engaged in virtual asset activities, such as brokers.

Specifically, a licence for a Regulated Activity in relation to virtual assets permits undertaking one or more virtual asset activities, including:

a) buying, selling or exercising any right in accepted virtual assets (whether as principal or agent);
b) managing accepted virtual assets belonging to another person;
c) making arrangements with a view to another person (whether as principal or agent) buying, selling or providing custody of accepted virtual assets;
d) marketing of accepted virtual assets;
e) advising on the merits of buying or selling of accepted virtual assets or any rights conferred by such buying or selling;
f) operating a Multilateral Trading Facility in relation to virtual assets; and/or
g) operating as a Virtual Asset custodian.

Firms wishing to apply for one of the above permissions can only do so in relation to "Accepted virtual assets". These virtual assets are the ones that fulfil the criteria prescribed by the FSRA. A list of accepted virtual assets is not publicly available. Each applicant must submit an application for each virtual asset they intend to offer, regardless of whether the FSRA may have accepted the virtual asset for another Authorised Firm.

As for now, there are 5 virtual asset firms launched in ADGM:

1. Matrix (operating a regulated virtual asset Multilateral Trading Facility and custody platform);
2. MidChains (operating a regulated virtual asset Multilateral Trading Facility and custody platform);
3. Hayvn (arranging deals in investments and providing custody for accepted virtual assets);
4. Seba Bank (advising on investments or credit, arranging credit and custody, and arranging deals in investments);
5. Yoshi markets (operating a regulated virtual asset Multilateral Trading Facility and custody platform).

Bahrain

The Bahraini framework has also the common financial center feature and is based on the UK financial legal framework. Bahrain adopted its DASPs and DA regulatory framework in 2019. Bahrain established a standalone crypto framework that is comprehensive, convenient in terms of navigation, has some commonalities with ADGM, but at the same time provides for many specific and tailored measures that address the risks of the DASP-related activities.

According to the Central Bank of Bahrain and Financial Institutions Law 2006 regulated crypto-asset services means the conduct of any or any combination of the following types of activities:

a) Reception and Transmission of order;
b) Execution of orders on behalf of clients;

c) Dealing on own account;
d) Portfolio Management;
e) Crypto-asset Custodian;
f) Investment Advice;
g) Crypto-asset exchange.

As of the date of this paper, there are 3 licensed companies in Bahrain:

1. Binance Bahrain B.S.C (other activities auxiliary to financial service activities - Crypto-asset services)
2. Rain Management W.L.L. (trading in accepted crypto-assets as agent; trading in accepted crypto-assets as principal; portfolio management; crypto-asset custody; investment advice)
3. Coinmena B.S.C. (trading in accepted crypto-assets as agent; portfolio management; crypto-asset custody; investment advice; trading in accepted crypto-assets as principal)

The United Arab Emirates (Virtual Asset Regulatory Authority)

On 7 February 2023, the Dubai Virtual Asset Regulatory Authority (VARA) issued the Virtual Assets and Related Activities Regulations 2023 (VARA Regulations) and accompanying Rulebooks which set out VARA's Virtual Asset Regime for the Emirate of Dubai (including its commercial freezones but excluding the Dubai International Financial Centre (DIFC)) in UAE.

Virtual assets are broadly defined as "a digital representation of value that may be digitally traded, transferred, or used as an exchange or payment tool, or for investment purposes. This includes virtual tokens, which are a digital representation of a set of rights that can be digitally offered and traded through a virtual asset platform, and any digital representation of any other value as determined by VARA".

The regulated virtual asset activities, which will require a licence from VARA are:

a) Advisory Services;
b) Broker-Dealer Services;
c) Custody Services;
d) Exchange Services;
e) Lending and Borrowing Services;
f) Payments and Remittances Services; and
g) VA Management and Investment Services.

During 2022, VARA has been working with established virtual asset service providers (VASPs) including Binance and Crypto.com on a minimum viable product program (MVP Program) to onboard VASPs into the jurisdiction.

VARA has also announced that it plans to only permit the MVP Program licensees to provide services to qualified and/or institutional investors in the initial stages, following which the VASPs will be able to progress to a full market product licence and permission to onboard retail clients.

Hex Trust and Crypto.com have officially launched its operations in Dubai after receiving the MVP Operational Licence from VARA, in February and March respectively.

Proposals

Based on the best practice analysis of the DIFC and ADGM, the following Regulated Activities are proposed to be allowed for carrying on, in or from the AIFC, in relation to Digital Assets:

(a) Dealing in Investments as Principal;
(b) Dealing in Investments as Agent;
(c) Managing Investments;
(d) Managing a Collective Investment Scheme;
(e) Providing Custody;
(f) Arranging Custody;
(g) Advising on Investments; and
(h) Arranging Deals in Investments.

After preliminary analysis conducted by the AFSA, it is proposed to introduce the following common requirements related to:

1. Authorisation of Digital Asset Service Providers, including the capital requirement and mandatory appointments applicable to Digital Asset Service Providers;
2. Implementing technology governance, controls and systems requirements;
3. Establishing appropriate internal policies and procedures, as well as public disclosure requirements;
4. Provision of key features document and disclosure of risks;
5. Reconciliation;
6. Investment limits and calculation of net assets for effective client management;
7. Prohibitions on marketing, facilitating investments, and certain activities related to Digital Assets;
8. Regular reporting and breach notification obligations.

Digital Asset Service Provider carrying on any one or more of the Regulated Activities in relation to Digital Assets should be subject to relevant provisions of AIFC Acts either directly or in respect of its officers and Employees who are Approved or Designated Individuals.

It is also proposed to introduce the following requirements for each Regulated Activity in relation to Digital assets:

1. Digital Asset Service Providers carrying on a Regulated Activity of Advising on Investments and Arranging Deals in Investments are proposed to ensure that the advice provided is free from misleading or false information, and they must verify factual information from reliable sources, while also assessing a diverse range of Digital Assets to meet the client's investment objectives;
2. Digital Asset Service Providers carrying on a Regulated Activity of Providing and Arranging Custody should comply with the applicable requirements for a proper digital wallet management. This includes ensuring resilient and compatible DLT applications, clear segregation of a client’s digital assets, proper cryptographic key management, providing contractual arrangements, making additional disclosures in order to strengthen security and protect client assets;

3. The requirements for Digital Asset Service Providers Managing Investments and a Collective Investment Scheme should include verification of information, providing transparent client reporting and valuation, implementation of risk management and due diligence measures, and maintaining confirmation notes.

4. Digital Asset Service Providers Dealing in Investments as Principal or Agent should also maintain confirmation notes that include information, that ensures transparency and clarity for clients regarding their investment transactions, and conduct appropriateness test.

Public consultation questions

In the course of public consultation, existing and potential market participants will be invited to comment on the following questions:

(1) AFSA invites comments on the draft Rules on Digital Asset Activities related to the Digital Asset Service Providers and consequential amendments.
(2) What is your view on the proposed capital requirements?
(3) What do you think about the proposed requirements in relation to the IT systems and technology governance?
(4) Do you agree with the proposed restrictions and prohibitions?

Outcomes

It is expected that the introduction of the Digital Asset Service Providers framework will help:
1) address and mitigate risks related to the Digital Asset Service Providers' activities;
2) support innovation and fair competition;
3) maintain the competitiveness of the AIFC on international financial and technological markets; and
4) provide investors with significant benefits in terms of access to cheaper, faster and safer financial services and asset management.

Annex 1

RULES APPLICABLE TO DIGITAL ASSET SERVICE PROVIDERS

This Part 3 applies to a Person carrying on, in or from the AIFC, one or more of the following Regulated Activities in relation to Digital Assets:

(a) Dealing in Investments as Principal;
(b) Dealing in Investments as Agent;
(c) Managing Investments;
(d) Managing a Collective Investment Scheme;
(e) Providing Custody;
(f) Arranging Custody;
(g) Advising on Investments; and
(h) Arranging Deals in Investments.

3.1. Authorisation of Digital Asset Service Providers

A Person wishing to carry on one or more of the Regulated Activities in relation to Digital Assets in or from the AIFC must be an Authorised Firm licensed by the AFSA.

3.2. Requirements for Digital Asset Service Providers

The AFSA may not grant authorisation or variation to carry on the Regulated Activities in relation to Digital Assets, except for Operating a Digital Asset Trading Facility, unless the applicant satisfies all of the following requirements:

(1) general authorisation requirements applicable to the applicant under the Framework Regulations and other applicable rules, and

(2) the applicant must ensure that it maintains at all times capital resources in the amount specified in Table 2 by reference to the activity that the Digital Asset Service Provider is authorised to conduct or, if it is authorised to conduct more than one such activity, the amount that is the higher or highest of the relevant amounts in Table 2.

Table 2

Regulated Activity	Capital requirement (USD)
Dealing in Investments as Principal, unless such activities are limited to matching client orders and the AFSA determines that it is appropriate in all the circumstances to apply a lower capital requirement	250,000
Dealing in Investments as Principal, where such activities are limited to matching client orders and the AFSA determines that it is appropriate in all the circumstances to apply a lower capital requirement than above	50,000
Dealing in Investments as Agent	50,000
Managing Investments	100,000
Managing a Collective Investment Scheme, which is an externally managed Exempt Fund and has an appointed Eligible Custodian, unless the appointment of an Eligible Custodian is not require	50,000
Managing a Collective Investment Scheme, which is a Non-Exempt Fund	150,000
Managing a Collective Investment Scheme, which is a Self-managed Fund and has an appointed Eligible Custodian, unless the appointment of an Eligible Custodian is not required due to the nature of the Fund and the type of assets which it holds	200,000

Managing a Collective Investment Scheme, which does not have an appointed Eligible Custodian, except where an Eligible Custodian is not required due to the nature of the Fund and type of assets which it holds	250,000
Providing Custody	250,000
Arranging Custody	10,000
Advising on Investments	10,000
Arranging Deals in Investments	10,000

Guidance:
A Digital Asset Service Provider may carry on the Regulated Activities only in relation to Digital Assets and may not carry on the Regulated Activities in relation to other Investments unless for circumstances which could be approved by the AFSA on a case-by-case basis.

3.3. Mandatory appointment

In addition to the mandatory appointments required by GEN 2.1., a Digital Asset Service Provider must appoint a Chief Information Technology Officer, who is an individual responsible for its ongoing information technology ("IT") operations, maintenance and security oversight to ensure that the Digital Asset Service Provider's IT systems are reliable and adequately protected from external attack or incident.

3.4. Technology governance, controls and security

3.4.1. Systems and controls

(1) A Digital Asset Service Provider must ensure that they implement systems and controls necessary to address the risks, including cybersecurity-related risks, to its business. The relevant systems and controls should take into account such factors that include but not limited to the nature, scale and complexity of the Digital Asset Service Provider's business, the diversity of its operations, the volume and size of its transactions and the level of risk inherent with its business.
(2) A Digital Asset Service Providers must have adequate systems and controls to enable it to calculate and monitor its capital resources and its compliance with the requirements in DAA 3.2.(2). The systems and controls must be in writing and must be appropriate for the nature, scale and complexity of the Digital Asset Service Provider's business and its risk profile.

3.4.2. Technology governance and risk assessment framework

(1) Digital Asset Service Providers must implement a technology governance and risk assessment framework which must be comprehensive and proportionate to the nature, scale, and complexity of the risks inherent in their business model.
(2) The technology governance and risk assessment framework must apply to all technologies relevant to a Digital Asset Service Provider's business and clearly set out the Digital Asset Service Provider's cybersecurity objectives, including the requirements for the competency of its relevant Employees and, as relevant, end users and clients and clearly defined systems and procedures necessary for managing risks.
(3) Digital Asset Service Providers must ensure that their technology governance and risk assessment is capable of determining the necessary processes and controls that they must implement in order to adequately mitigate any risks identified. In particular, Digital Asset Service Providers must ensure that their technology governance and risk assessment framework includes consideration of international standards and industry best practice codes.
(4) Digital Asset Service Providers must ensure that their technology governance and risk assessment framework addresses appropriate governance policies and system development controls, such as a development, maintenance and testing process for technology systems and operations controls, back-up controls, capacity and performance planning and availability testing.

3.4.3. Cyber-security matters

A Digital Asset Service Provider must take reasonable steps to ensure that its IT systems are reliable and adequately protected from external attack or incident.

3.4.4. Cyber-security policy

(1) A Digital Asset Service Provider must create and implement a policy which outline their procedures for the protection of its electronic systems.

(2) A Digital Asset Service Provider must ensure that its cyber-security policy is reviewed at least on an annual basis by its Chief Information Technology Officer.

(3) The cyber-security policy must, as a minimum, address the following areas:

(a) information security;

(b) data governance and classification;

(c) access controls;

(d) business continuity and disaster recovery planning and resources;

(e) capacity and performance planning;

(f) systems operations and availability concerns;

(g) systems and network security, consensus protocol methodology, code and smart contract validation and audit processes;

(h) systems and application development and quality assurance;

(i) physical security and environmental controls, including but not limited to procedures around access to premises and systems;

(j) customer data privacy;

(i) procedures regarding their facilitation of Digital Asset transactions initiated by a Client including, but not limited to, considering multi-factor authentication or any better standard for Digital Asset transactions that—

(i) exceed transaction limits set by the Client, such as accumulative transaction limits over a period of time; and

(ii) are initiated after a change of personal details by the Client, such as the address of a Digital wallet;

(j) procedures regarding Client authentication and session controls including, but not limited to, the maximum incorrect attempts for entering a password, appropriate time-out controls and password validity periods;

(k) procedures establishing adequate authentication checks when a change to a Client's account information or contact details is requested;

(l) vendor and third-party service provider management;

(m) monitoring and implementing changes to core protocols not directly controlled by the Digital Asset Service Provider, as applicable;

(n) incident response, including but not limited to, root cause analysis and rectification activities to prevent reoccurrence;

(o) governance framework and escalation procedures for effective decision-making and proper management and control of risks and emergency incidents, including but not limited to responses to ransomware and other forms of cyberattacks; and

(p) hardware and infrastructure standards, including but not limited to network lockdown, services/desktop security and firewall standards.

3.4.5. Cryptographic keys and Digital wallets management

(1) A Digital Asset Service Provider must ensure that its technology governance and risk assessment framework addresses, to the extent necessary, the generation of cryptographic keys and Digital wallets, the signing and approval of transactions, the storage of cryptographic keys and seed phrases, Digital wallets creation and management thereof.

(2) A Digital Asset Service Provider must:

(a) safeguard access to Digital Assets in accordance with industry best practices and, in particular, ensure that there is no single point of failure in the Digital Asset Service Provider's access to, or knowledge of, Digital Assets held by the Digital Asset Service Provider;

(b) adopt industry best practices for storing the private keys of Clients, including ensuring that keys stored online or in any one physical location are insufficient to conduct a Digital Asset transaction, unless appropriate controls are in place to render physical access insufficient to conduct such Digital Asset transaction;

(c) ensure that backups of the key and seed phrases are stored in a separate location from the primary key and/or seed phrase;

(d) adopt strict access management controls to manage access to keys, including an audit log detailing each change of access to keys;

(e) adopt procedures designed to immediately revoke a key signatory's access.

(3) A Digital Asset Service Provider must:

(a) ensure that the key generation process ensures that revoked signatories do not have access to the backup seed phrase or knowledge of the phrase used in the key's creation;
(b) perform internal audits on a quarterly basis concerning the removal of user access by reviewing access logs and verifying access as appropriate;
(c) implement and maintain a procedure for documenting the onboarding and offboarding of staff;
(d) implement and maintain a procedure for documenting a Digital Asset Service Provider's permission to grant or revoke access to each role in its key management system; and
(e) regularly assess the security of its IT systems or software integrations with external parties and ensure that the appropriate safeguards are implemented in order to mitigate all relevant risks.
(4) Digital Asset Service Providers should provide information to Clients on measures they can take to protect their keys and/or seed phrases from misuse or unauthorised access, and the consequences of sharing their private keys and other security information.
(5) Digital Asset Service Providers must ensure that access to their systems and data may only be granted to individuals with a demonstrable business need and implement safeguards to ensure the proper identification of all individuals, including the maintenance of an access log.

3.4.6. On-going monitoring
For the purposes of meeting the requirement in DAA 3.4.1, a Digital Asset Service Provider must have adequate procedures and arrangements for the evaluation, selection and on-going maintenance and monitoring of its IT systems. Such procedures and arrangements must, at a minimum, provide for:
(a) problem management and system change;
(b) testing IT systems before live operations in accordance with the requirements in DAA 3.4.7;
(c) real time monitoring and reporting on system performance, availability and integrity; and
(d) adequate measures to ensure:
(i) the IT systems are resilient and not prone to failure;
(ii) business continuity in the event that an IT system fails;
(iii) protection of the IT systems from damage, tampering, misuse or unauthorised access; and
(iv) the integrity of data forming part of, or being processed through, IT systems.

3.4.7. Testing and audit of technology systems
(1) A Digital Asset Service Provider must, before commencing live operation of its IT systems or any updates thereto, use development and testing methodologies in line with internationally accepted testing standards in order to test the viability and effectiveness of such systems. For this purpose, the testing must be adequate for the Digital Asset Service Provider to obtain reasonable assurance that, among other things:
(a) the systems enable it to comply with all the applicable requirements on an on-going basis;
(b) the systems can continue to operate effectively in stressed market conditions;
(c) the systems have sufficient electronic capacity to accommodate reasonably foreseeable volumes of messaging and orders; and
(d) any risk management controls embedded within the systems, such as generating automatic error reports, work as intended.
(2) A Digital Asset Service Provider is required to undergo a qualified independent third-party technology governance and IT audit to conduct vulnerability assessments and penetration testing at least on an annual basis.
(2) A Digital Asset Service Providers must engage a qualified independent third-party auditor prior to the introduction of any new systems, applications and products.
(3) A Digital Asset Service Provider must provide the results of technology governance and IT assessments and tests to the AFSA upon its request.

3.4.8. Technology audit reports
(1) This Rule applies to an Authorised Firm that:
(a) holds or controls Digital Assets;
(b) relies on DLT or similar technology to carry on one or more of the following Regulated Activities in relation to Digital Assets:
(i) Dealing in Investments as Principal;
(ii) Dealing in Investments as Agent;
(iii) Arranging Deals in Investments;
(iv) Managing Investments;
(v) Advising on Investments;

(vi) Providing Custody; or
(vii) Arranging Custody; or
(c) is Managing a Collective Investment Scheme where:
(i) Units of the Fund are Security Tokens; or
(ii) 10% or more of the gross asset value of the Fund Property of the Fund consists of Digital Assets.
(2) The Authorised Firm must:
(a) appoint a suitably qualified independent third-party professional to:
(i) carry out an annual audit of the Authorised Firm's compliance with the technology resources and governance requirements that apply to it; and
(ii) produce a written report which sets out the methodology and results of that annual audit, confirms whether the requirements referred to in DAA 3.4.8. (i) have been met and lists any recommendations or areas of concern;
(b) submit to the AFSA a copy of the report referred to in DAA 3.4.8. (a)(ii) within 4 months of the Authorised Firm's financial year end; and
(c) be able to satisfy the AFSA that the independent third party professional appointed to carry out the annual audit has the relevant expertise to do so, and that the Authorised Firm has done proper due diligence to satisfy itself of that fact.
(3) A Digital wallet Service Provider must ensure that the report required under DAA 3.4.8 (a)(ii) includes confirmation as to whether it has complied with the requirements in DAA 3.5.1.

Guidance:
Credentials which indicate a qualified independent third-party auditor is suitable to conduct audit of technology governance and IT systems may include:
(1) designation as a Certified Information Systems Auditor (CISA) or Certified Information Security Manager (CISM) by the Information Systems Audit and Control Association (ISACA);
(2) designation as a Certified Information Systems Security Professional (CISSP) by the International Information System Security Certification Consortium (ISC); or
(3) accreditation by a recognised and reputable body to certify compliance with relevant ISO/IEC 27000 series standards; or
(4) accreditation by the relevant body to certify compliance with the Kazakhstani standards in the area of information (cyber) security.

3.5. Policies, procedures, and public disclosures

3.5.1. Policies and procedures required for Digital Asset Service Providers

(1) Digital Asset Service Providers carrying on a Regulated Activity of Advising on Investments must establish, implement and enforce appropriate written internal policies and procedures relating to the following:
(a) how they ensure the independent basis of their advice;
(b) how they ensure all Directors and Employees providing the relevant advice are sufficiently competent;
(c) such other policies and procedures as the AFSA may require from time to time.
(2) Digital Asset Service Providers carrying on Regulated Activities of Dealing in Investments as Principal or Agent must establish, implement and enforce appropriate written internal policies and procedures relating to the following:
(a) the prohibition, detection, prevention and/or deterrence of market offences and any other abusive practices within their business or using their services including, but not limited to, relevant internal rules, compliance programmes, sanctioning policies and powers;
(b) Execution and routing of Client orders;
(c) the ability of Clients to have access to and withdraw their Digital Assets including, but not limited to, during periods of high uncertainty and/or extreme volatility; and
(d) such other policies and procedures as the AFSA may require from time to time.
(3) Digital Asset Service Providers carrying on a Regulated Activity of Providing Custody must establish, implement and enforce appropriate written internal policies and procedures relating to the following:
(a) the ability of Clients to have access to and withdraw their Digital Assets including, but not limited to, during periods of high uncertainty and/or extreme volatility; and
(b) such other policies and procedures as the AFSA may require from time to time.
(4) Digital Asset Service Providers carrying on a Regulated Activity of Managing Investments must establish, implement and enforce appropriate written internal policies and procedures relating to the following:

(a) the ability of Clients to have access to and withdraw their Digital Assets including, but not limited to, during periods of high uncertainty and/or extreme volatility;
(b) their assessment of Client suitability for relevant products or services, including but not limited to the nature, features, costs and risks of investment services, Digital Assets or other financial instruments selected for their Clients, while taking into account cost and complexity;
(c) how they ensure all Directors and Employees Managing Investments to Clients are sufficiently competent; and
(d) such other policies and procedures as the AFSA may require from time to time.
(5) All Digital Asset Service Providers specified in (1) to (4) must assess and, in any case, at least yearly review the effectiveness of their policies and procedures and take appropriate measures to address any deficiencies.

3.5.2. Public disclosures

(1) All Digital Asset Service Providers specified in (1) to (4) in DAA 3.5.1. must publish on their website in a prominent place or make available by other publicly accessible means:
(a) a detailed description of any actual or potential conflicts of interest arising out of their activities, and how these are managed; and
(b) their policies and procedures relating to data privacy, whistleblowing and handling of Client complaints.
(2) In addition to (1), Digital Asset Service Providers carrying on a Regulated Activity of Advising on Investments must publish on their website in a prominent place or make available by other publicly accessible means:
(a) a statement of whether the Digital Asset Service Provider refers or introduces Clients to other Persons including, but not limited to, other Digital Asset Service Providers, and if so, a description of the terms of such arrangements, and the monetary or non-monetary benefits received by the Digital Asset Service Provider, including by way of reciprocation for any service or business; and
(b) a statement of whether the Digital Asset Service Provider has accounts, funds or Digital Assets maintained by a third party and if so, provide the identity of that third party.
(3) In addition to (1), Digital Asset Service Providers carrying on Regulated Activities of Dealing in Investments as Principal or Agent must publish on their website in a prominent place or make available by other publicly accessible means:
(a) a statement as to the Digital Asset Service Provider's arrangements for the protection of Clients' ownership of assets held by the Digital Asset Service Provider;
(b) a statement of whether the Digital Asset Service Provider refers or introduces Clients to other Persons including, but not limited to, other Digital Asset Service Providers and, if so, a description of the terms of such arrangements and the monetary or non-monetary benefits received by the Digital Asset Service Provider, including by way of reciprocation for any service or business; and
(c) a statement of whether the Digital Asset Service Provider has accounts, funds or Digital Assets maintained by a third party and if so, provide the identity of that third party.
(4) In addition to (1), Digital Asset Service Providers carrying on a Regulated Activity of Providing Custody must publish on their website in a prominent place or make available by other publicly accessible means a statement of whether the Digital Asset Service Provider has accounts, funds or Digital Assets maintained by a third party and if so, provide the identity of that third party.
(5) In addition to (1), Digital Asset Service Providers carrying on a Regulated Activity of Managing Investments must publish on their website in a prominent place or make available by other publicly accessible means:
(a) a statement as to the ability of clients to have access to and withdraw their Digital Assets, particularly in times of extreme volatility;
(b) a statement as to the Digital Asset Service Provider's arrangements for the protection of Clients' assets held by the Digital Asset Service Provider and how it determines uses of Client Digital Assets including but not limited to a detailed description of such uses;
(c) a statement as to how they protect Client Digital Assets from counterparty risk;
(d) a statement as to how in the course of Managing Investments, Client Digital Assets are used and how Clients' interests in respect of those Digital Assets are thereby respected;
(e) a statement explaining that Client Digital Assets used by the Digital Asset Service Provider in the course of Managing Investments may be at risk, including the types and nature of such risks, and a statement on the likelihood and severity of any losses which may be suffered;

(f) a statement in relation to order execution by the Digital Asset Service Provider;
(g) a statement as to how liquidity risk is managed; and
(h) such other information as the AFSA may require from time to time.

3.6. Requirements for Digital Asset Service Providers Advising on Investments and Arranging Deals in Investments

Guidance: A Digital Asset Service Provider which carries on a Regulated Activity of Advising on Investments in relation to Digital Assets is an Authorised Firm to which the following provisions of the GEN, COB, and AML are applicable either directly or in respect of its officers and Employees who are Approved or Designated Individuals:
AML (in whole);
Chapter 2 (Client classification) of the COB;
Chapter 3 (Communication with Clients and Financial Promotions) of the COB;
Chapter 4 (Key information and client agreement) of the COB;
COB 5.2 (Suitability assessment) of the COB;
Chapter 7 (Conflicts of interest) of the COB;
Chapter 10 (Investment research) of the COB;
Chapter 15 (Complaints handling and dispute resolution) of the COB;
Chapter 16 (Record keeping and internal audit) of the COB;
Chapter 2 (Controlled and Designated Functions) of the GEN;
Chapter 3 (Control of Authorised Persons) of the GEN;
Chapter 4 (Core Principles) of the GEN;
Chapter 5 (Systems and Controls) of the GEN;
Chapter 6 (Supervision) of the GEN; and
Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC (in whole).

3.6.1. Verification of information

(1) In addition to requirements set out in Chapter 3 of the COB, Digital Asset Service Providers Advising on Investments must provide advice which does not contain statements, promises, forecasts or other types of information which they know or suspect to be misleading, false or deceptive or which they should have reasonably known to be misleading, false or deceptive at the time of making such statement, promise or forecast.
(2) Prior to making any statement, promise or forecast, a Digital Asset Service Provider Advising on Investments must verify factual information against appropriate and reliable source materials and must use all reasonable endeavours to verify the continued accuracy of such information.

3.6.2. Methodology

A Digital Asset Service Provider in the course of Advising on Investments must assess a broad range of Digital Assets available to the Client which should be sufficiently diverse such that the Client's investment objectives are met.

3.6.3. Appropriateness test

A Digital Asset Service Provider Arranging Deals in Investments must not carry on a Regulated Activity with or for a Retail Client, who is a non-resident of the Republic of Kazakhstan, unless the Digital Asset Service Provider has carried out an appropriateness test of the Person and formed a reasonable view that the Person has:
(a) adequate skills and expertise to understand the risks involved in trading in Digital Assets or Digital Asset Derivatives (as the case may be); and
(b) the ability to absorb potentially significant losses resulting from trading in Digital Assets or Digital Asset Derivatives (as the case may be).

Guidance:
(1) To form a reasonable view referred to in DAA 3.6.3. in relation to a Person, a Digital Asset Service Provider should consider issues such as whether the Person:
(a) has sufficient knowledge and experience relating to the type of a Digital Asset or Digital Asset Derivative offered, having regard to such factors as:

(i) how often and in what volumes that Person has traded in the relevant type of a Digital Asset or Digital Asset Derivative; and
(ii) the Person's relevant qualifications, profession or former profession;
(b) understands the characteristics and risks relating to Digital Assets or Digital Asset Derivatives, and the volatility of their prices;
(c) understands the impact of leverage, due to which, there is potential to make significant losses in trading in Digital Assets or Digital Asset Derivatives; and
(d) has the ability, particularly in terms of net assets and liquidity available to the Person, to absorb and manage any losses that may result from trading in the Digital Assets or Digital Asset Derivatives offered.
(2) To be able to demonstrate to the AFSA that it complies with DAA 3.6.3., a Digital Asset Service Provider should have in place systems and controls that include:
(a) pre-determined and clear criteria against which a Retail Client's ability to trade in Digital Assets or Digital Asset Derivatives can be assessed;
(b) adequate records to demonstrate that the Digital Asset Service Provider has undertaken the appropriateness test for each Retail Client; and
(c) in the case of an existing Retail Client with whom the Digital Asset Service Provider has previously traded in Digital Assets or Digital Asset Derivatives, procedures to undertake a fresh appropriateness test if:
(i) a new Digital Asset or Digital Asset Derivative with a materially different risk profile is offered to the Retail Client; or
(ii) there has been a material change in the Retail Client's circumstances.
(3) If a Digital Asset Trading Facility Operator forms the view that it is not appropriate for a Person to trade in Digital Assets or Digital Asset Derivatives, the Digital Asset Trading Facility Operator should refrain from offering that service to the Person. As a matter of good practice, the Digital Asset Trading Facility Operator should inform the Person of its decision.

3.7. Requirements for Digital Asset Service Providers Providing and Arranging Custody

Guidance: A Digital Asset Service Provider which carries on a Regulated Activity of Providing Custody in relation to Digital Assets is an Authorised Firm to which the following provisions of the GEN, COB, and AML are applicable either directly or in respect of its officers and Employees who are Approved or Designated Individuals:
AML (in whole);
Chapter 2 (Client classification) of the COB;
Chapter 3 (Communication with Clients and Financial Promotions) of the COB;
Chapter 4 (Key information and client agreement) of the COB;
Chapter 7 (Conflicts of interest) of the COB;
Chapter 8 (Client Assets) of the COB;
Chapter 15 (Complaints handling and dispute resolution) of the COB;
Chapter 16 (Record keeping and internal audit) of the COB;
Chapter 2 (Controlled and Designated Functions) of the GEN;
Chapter 3 (Control of Authorised Persons) of the GEN;
Chapter 4 (Core Principles) of the GEN;
Chapter 5 (Systems and Controls) of the GEN;
Chapter 6 (Supervision) of the GEN; and
Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC (in whole).

A Digital Asset Service Provider which carries on a Regulated Activity of Arranging Custody in relation to Digital Assets is an Authorised Firm to which the following provisions of the GEN, COB, and AML are applicable either directly or in respect of its officers and Employees who are Approved or Designated Individuals:
AML (in whole);
Chapter 2 (Client classification) of the COB;
COB 8.3.7 (on assessing the suitability of Third Party Account Providers);
COB 8.3.13 (on disclosure);
COB 8.3.14(2) (on client reporting);
COB 8.3.15 (on record keeping);

Chapter 3 (Control of Authorised Persons) of the GEN;
Chapter 4 (Core Principles) of the GEN;
Chapter 5 (Systems and Controls) of the GEN; and
Chapter 6 (Supervision) of the GEN.

3.7.1. Requirements for Digital Asset Service Providers Providing Custody of Digital Assets

(1) A Digital wallet Service Provider must ensure that:
(a) any DLT application it uses in Providing Custody of Digital Assets is resilient, reliable and compatible with any relevant facility on which the Digital Assets are traded or cleared;
(b) it is able to clearly identify and segregate Digital Assets belonging to different Clients; and
(c) it has in place appropriate procedures to enable it to confirm Client instructions and transactions, maintain appropriate records and data relating to those instructions and transactions and to conduct a reconciliation of those transactions at appropriate intervals.
(2) A Digital wallet Service Provider must ensure that, in developing and using DLT applications and other technology to Provide Custody of Digital Assets:
(a) the architecture of any Digital wallet used adequately addresses compatibility issues and associated risks;
(b) the technology used and its associated procedures have adequate security measures (including cyber security) to enable the safe storage and transmission of data relating to the Digital Assets;
(c) the security and integrity of cryptographic keys are maintained through the use of that technology, taking into account the password protection and methods of encryption used;
(d) there are adequate measures to address any risks specific to the methods of usage and storage of cryptographic keys (or their equivalent) available under the DLT application used; and
(e) the technology is compatible with the procedures and protocols built into the relevant rules or equivalent procedures and protocols on any facility on which the Digital Assets are traded or cleared or both traded and cleared.
(3) Digital Assets held by the Digital Asset Service Provider Providing Custody are not depository liabilities or assets of the Digital Asset Service Provider and must hold them on trust.

Guidance:

Where an Authorised Person which is a Digital wallet Service Provider delegates any functions to a Third Party Digital wallet Service provider, it must ensure that the delegate fully complies with the requirements of DAA 3.7.1. The outsourcing and delegation requirements of GEN 5.2.

3.7.2. Digital wallet management

(1) Requirements in relation to Hot and Cold Digital wallet storage.
(a) A Digital wallet Service Provider must at all times maintain appropriate certifications as may be required under industry best practices applicable to the safekeeping of Digital Assets.
(b) A Digital wallet Service Provider should conduct a risk-based analysis to determine the method of Digital Asset storage including different types of Digital wallets.
(c) A Digital wallet Service Provider should document in detail the methodologies and behaviour determining the transfer of Digital Assets between different types of Digital wallets. The mechanisms for transfer between different types of Digital wallets should be well documented and subject to internal controls and audits performed by an independent third-party auditor in ensuring compliance with DAA 3.6.2 (1).
(2) Seed or key generation, storage, and use.
(a) To ensure a secure generation mechanism, a Digital wallet Service Provider must use industry best standards to create the seed, asymmetric private and public key combinations, or other similar mechanisms.
(b) A Digital wallet Service Provider must consider all risks associated with producing a private key or seed for a signatory including whether the signatory should be involved in the generation process or whether creators of the seed, private key, or other similar mechanism should be prohibited from cryptographically signing any transaction or from having access to any relevant systems.
(c) A Digital wallet Service Provider must adopt industry best practices when using encryption and secure device storage for a Client's private keys when not in use.
(d) A Digital wallet Service Provider must ensure that any keys stored online or in one physical location are not capable of conducting a Digital Asset transaction, unless appropriate controls are in place to ensure that physical access itself by an individual is insufficient to conduct a transaction.

(e) All key and seed backups must be stored in a separate location from the primary key and seed. Key and seed backups must be stored with encryption at least equal to the encryption used to protect the primary seed and key.
(f) Digital wallet Service Providers must mitigate the risk of collusion between all authorised parties or signatories who are able to authorise the movement, transfer or withdrawal of Virtual Assets held under custody on behalf of clients. The risk of collusion and other internal points of failure should be addressed during recurring operational risk assessments.
(3) Lost or stolen keys.
(1) Digital wallet Service Providers must establish and maintain effective policies and procedures in the event that any seed or cryptographic keys of any Digital wallet are lost or otherwise compromised.
(2) The policy and procedures must address matters including but not limited to:
(a) recovery of affected Digital Assets;
(b) timely communications with all clients and counterparties regarding consequences arising from relevant incidents and measures being taken to remedy such consequences;
(c) cooperation with law enforcement agencies and regulatory bodies; and
(d) if applicable, preparation of winding down arrangements and public disclosure of such arrangements.

3.7.3. Contractual arrangement

A Digital Asset Service Provider that is Providing Custody for a Client should provide such activity based on a contractual arrangement. Under such an arrangement a Client is lawfully in control of, or entitled to control, a Digital Asset, transfers control of the Digital Asset to a Digital Asset Service Provider solely for the purpose of receiving custody services and does not in any way transfer to the Digital Asset Service Provider any legal interest in the Digital Asset or any discretionary authority not stated in the Client Agreement or otherwise agreed to by the Client.

3.7.4. Additional disclosure requirements

Before entering into an initial transaction for, on behalf of, or with a Client, a Digital wallet Service Provider must disclose in a clear, fair and not misleading manner:
(a) all terms, conditions and risks relating to the Digital Assets that have been admitted to trading and/or is the subject of the transaction;
(b) all material risks associated with its products, services and activities; and
(c) all details on the amount and the purpose of any premiums, fees, charges or taxes payable by the Client.

3.7.5. Additional information for a Digital Asset Service Provider Providing Custody of Digital Assets

A Digital Asset Service Provider Providing Custody of Digital Assets must include in the Client Agreement:
(a) a breakdown of all fees and charges payable for a transfer of Digital Assets (a “transfer”) and when they are charged;
(b) the information is required to carry out a transfer;
(c) the form and procedures for giving consent to a transfer;
(d) an indication of the time it will normally take to carry out a transfer;
(e) details of when a transfer will be considered to be complete;
(f) how, and in what form, information and communications relating to transfer services will be provided to the Client, including the timing and frequency of communications and the language used and technical requirements for the Client’s equipment and software to receive the communications;
(g) clear policies and procedures relating to unauthorised or incorrectly executed transfers, including the Client is and is not entitled to redress;
(h) clear policies and procedures relating to situations where the holding or transfer of Digital Assets may have been compromised, such as if there has been hacking, theft or fraud; and
(i) details of the procedures the Authorised Firm will follow to contact the Client if there has been suspected or actual hacking, theft or fraud.

3.7.6. Client accounts in relation to Client Investments or Digital Assets

(1) A Digital Asset Service Provider which Provides Custody or holds or controls Client Investments or Client Digital Assets must register or record all Safe Custody Investments in the legal title of:
(a) a Client Account; or
(b) the Digital Asset Service Provider where, due to the nature of the law or market practice, it is not feasible to do otherwise.
(2) A Client Account in relation to Client Investments or Client Digital Assets is an account which:
(a) is held with a Third Party Agent or by a Digital Asset Service Provider which is authorised under its Licence to carry on the Regulated Activity of Providing Custody;
(b) is established to hold Client Assets;
(c) when held by a Third Party Agent, is maintained in the name of;
(i) if a Domestic Firm, the Digital Asset Service Provider; or
(ii) if not a Domestic Firm, a Nominee Company controlled by the Digital Asset Service Provider; and
(d) includes the words 'Client Account' in its title.
(3) A Digital Asset Service Provider must maintain a master list of all Client Accounts which must detail:
(a) the name of the account;
(b) the account number;
(c) the location of the account;
(d) whether the account is currently open or closed; and
(e) the date of opening or closure.
(4) A Digital Asset Service Provider must not use a Client's Safe Custody Investments or Safe Custody Digital Assets for its own purpose or that of another Person without that Client's prior written consent.
(5) A Digital Asset Service Provider which intends to use a Client's Safe Custody Investments or Safe Custody Digital Assets Tokens for its own purpose or that of another Person, must have systems and controls in place to ensure that:
(a) it obtains that Client's prior written consent;
(b) adequate records are maintained to protect Safe Custody Investments or Safe Custody Digital Assets which are applied as collateral or used for stock lending activities;
(c) the equivalent assets are returned to the Client Account of the Client; and
(d) the Client is not disadvantaged by the use of his Safe Custody Investments.

3.7.7. Client disclosure

(1) Before an Authorised Firm Arranges Custody for a Client it must disclose to that Client, if applicable, that the Client's Safe Custody Investments or Safe Custody Crypto Tokens may be held in a jurisdiction outside the DIFC and the market practices, insolvency and legal regime applicable in that jurisdiction may differ from the regime applicable in the DIFC.
(2) Before an Authorised Firm Provides Custody for a Client it must disclose to the Client on whose behalf the Safe Custody Investments or Safe Custody Crypto Tokens will be held:
(a) a statement that the Client is subject to the protections conferred by the Safe Custody Provisions;
(b) the arrangements for recording and registering Safe Custody Investments or Safe Custody Crypto Tokens, claiming and receiving dividends and other entitlements and interest and the giving and receiving instructions relating to those Safe Custody Investments or Safe Custody Crypto Tokens;
(c) the obligations the Authorised Firm will have to the Client in relation to exercising rights on behalf of the Client;
(d) the basis and any terms governing the way in which Safe Custody Investments will be held, including any rights which the Authorised Firm may have to realise Safe Custody Investments or Safe Custody Crypto Tokens held on behalf of the Client in satisfaction of a default by the Client;
(e) the method and frequency upon which the Authorised Firm will report to the Client in relation to his Safe Custody Investments or Safe Custody Crypto Tokens;
(f) if applicable, a statement that the Authorised Firm intends to mix Safe Custody Investments or Safe Custody Crypto Tokens with those of other Clients;
(g) if applicable, a statement that the Client's Safe Custody Investments or Safe Custody Crypto Tokens may be held in a jurisdiction outside the DIFC and the market practices, insolvency and legal regime applicable in that jurisdiction may differ from the regime applicable in the DIFC;
(h) if applicable, a statement that the Authorised Firm holds or intends to hold Safe Custody Investments or Safe Custody Crypto Tokens in a Client Account with a Third Party Agent which is in the same Group as the Authorised Firm; and
(i) the extent of the Authorised Firm's liability in the event of default by a Third Party Agent.

3.7.8. Client reporting

(1) An Authorised Firm which Provides Custody or which holds or controls Client Investments or Client Crypto Tokens for a Client must send a statement to a Retail Client at least every six months or in the case of a Professional Client at other intervals as agreed in writing with the Professional Client.
(2) The statement must include:
(a) a list of that Client's Safe Custody Investments or Safe Custody Crypto Tokens as at the date of reporting;
(b) a list of that Client's Collateral and the market value of that Collateral as at the date of reporting; and
(c) details of any Client Money held by the Authorised Firm as at the date of reporting.
(3) The statement sent to the Client must be prepared within 25 business days of the statement date.

3.7.9. Recording, registration and holding requirements
(1) A Digital Asset Service Provider which Provides Custody or holds or controls Client Investments or Client Digital Assets must ensure that Safe Custody Digital Assets are recorded, registered and held in an appropriate manner to safeguard and control such property.
(2) A Digital Asset Service Provider which Provides Custody or holds or controls Client Investments or Client Crypto Tokens must record, register and hold Safe Custody Investments separately from its own Investments.

3.8. Requirements for Digital Asset Service Providers Managing Investments and a Collective Investment Scheme

Guidance: A Digital Asset Service Provider which carries on a Regulated Activity of Managing Investments in relation to Digital Assets is an Authorised Firm to which the following provisions of the GEN, COB, and AML are applicable either directly or in respect of its officers and Employees who are Approved or Designated Individuals:
AML (in whole);
Chapter 2 (Client classification) of the COB;
Chapter 3 (Communication with Clients and Financial Promotions) of the COB;
Chapter 4 (Key information and client agreement) of the COB;
COB 5.2 (Suitability assessment);
Chapter 7 (Conflicts of interest) of the COB;
Chapter 15 (Complaints handling and dispute resolution) of the COB;
Chapter 16 (Record keeping and internal audit) of the COB;
Chapter 2 (Controlled and Designated Functions) of the GEN;
Chapter 3 (Control of Authorised Persons) of the GEN;
Chapter 4 (Core Principles) of the GEN;
Chapter 5 (Systems and Controls) of the GEN;
Chapter 6 (Supervision) of the GEN; and
Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC (in whole).

A Digital Asset Service Provider which carries on a Regulated Activity of Managing a Collective Investment Scheme in relation to Digital Assets is an Authorised Firm to which the following provisions of the GEN, COB, and AML are applicable either directly or in respect of its officers and Employees who are Approved or Designated Individuals:
AML (in whole);
Chapter 2 (Client classification) of the COB;
Chapter 3 (Communication with Clients and Financial Promotions) of the COB;
Chapter 4 (Key information and client agreement) of the COB;
Chapter 7 (Conflicts of interest) of the COB;
Chapter 15 (Complaints handling and dispute resolution) of the COB;
Chapter 16 (Record keeping and internal audit) of the COB;
Chapter 2 (Controlled and Designated Functions) of the GEN;
Chapter 3 (Control of Authorised Persons) of the GEN;
Chapter 4 (Core Principles) of the GEN;
Chapter 5 (Systems and Controls) of the GEN;
Chapter 6 (Supervision) of the GEN; and

Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC (in whole).

3.8.1. Verification of information

(1) In addition to requirements set out in Chapter 3 of the COB, Digital Asset Service Providers Managing Investments and/or a Collective Investment Scheme must not provide statements, promises, forecasts or other types of information which they know or suspect to be misleading, false or deceptive or which they should have reasonably known to be misleading, false or deceptive at the time of making such statement, promise or forecast.

(2) Prior to making any statement, promise or forecast, Digital Asset Service Providers Managing Investments and/or a Collective Investment Scheme must verify factual information against appropriate and reliable source materials and must use all reasonable endeavours to verify the continued accuracy of such information.

3.8.2. Client reporting and valuation

(1) Digital Asset Service Providers Managing Investments and/or a Collective Investment Scheme must, at least monthly, provide to each of their Clients a written statement containing the following information:

(a) the total value of Digital Assets in a Client's account;

(b) all transactions entered into between the Digital Asset Service Provider and the client in the reporting period; and

(c) the change in amount and valuation of Digital Assets in a Client's account [both total and during the reporting period].

(2) Digital Asset Service Providers Managing Investments and/or a Collective Investment Scheme must ensure that all assets under management are subject to ongoing independent valuation.

(3) Digital Asset Service Providers Managing Investments and/or a Collective Investment Scheme must have comprehensive and well documented valuation policies and procedures in place to ensure the production of timely and accurate valuation in accordance with DAA 3.7.2. (1).

3.8.3. Risk management and due diligence

(1) Digital Asset Service Providers Managing Investments and/or a Collective Investment Scheme must ensure that liquidity risk and market risk are each monitored and tested regularly, and appropriate measures put in place as required to address any such risk in a prompt manner.

(2) All such risk management and due diligence must be audited by an independent third party on an annual basis and provided to the AFSA upon request.

3.8.4. Content of confirmation notes

For the purposes of COB 9.1.3., a Digital Asset Service Provider Managing a Collective Investment Scheme must include the following general information:

(a) the Digital Asset Service Provider's name and address;

(b) whether the Digital Asset Service Provider executed the Transaction as principal or agent;

(c) the Client's name, account number or other identifier;

(d) a description of the Digital Asset;

(e) whether the Transaction is a sale or purchase;

(f) the price or unit price at which the Transaction was executed;

(g) if applicable, a statement that the Transaction was executed on an execution-only basis;

(h) the date and time of the Transaction;

(i) the total amount payable and the date on which it is due;

(j) the amount of the Digital Asset Service Provider charges in connection with the Transaction, including Commission charges and the amount of any Mark-up or Mark-down, Fees, taxes or duties;

(k) the amount or basis of any charges shared with another Person or statement that this will be made available on request; and

(l) at statement that the price at which the Transaction has been Executed is on a Historic Price or Forward Price basis, as the case may be.

(2) A Digital Asset Service Provider may combine items (f) and (j) above in respect of a Transaction where the Client has requested a note showing a single price combining both of these items.

3.9. Requirements for Digital Asset Service Providers Dealing in Investments as Principal or Agent

Guidance: A Digital Asset Service Provider which carries on a Regulated Activity of Dealing in Investments as Principal or Agent in relation to Digital Assets is an Authorised Firm to which the following provisions of the GEN, COB, and AML are applicable either directly or in respect of its officers and Employees who are Approved or Designated Individuals:
AML (in whole);
Chapter 2 (Client classification) of the COB;
Chapter 3 (Communication with Clients and Financial Promotions) of the COB;
Chapter 4 (Key information and client agreement) of the COB;
COB 5.3 (Appropriateness assessment);
Chapter 6 (Order execution and order handling) of the COB;
Chapter 7 (Conflicts of interest) of the COB;
Chapter 9 (Reporting to Clients) of the COB;
Chapter 15 (Complaints handling and dispute resolution) of the COB;
Chapter 16 (Record keeping and internal audit) of the COB;
Chapter 2 (Controlled and Designated Functions) of the GEN;
Chapter 3 (Control of Authorised Persons) of the GEN;
Chapter 4 (Core Principles) of the GEN;
Chapter 5 (Systems and Controls) of the GEN;
Chapter 6 (Supervision) of the GEN; and
Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC (in whole).

3.9.1. Content of confirmation notes

For the purposes of COB 9.1.3., a Digital Asset Service Provider must include the following general information:
(a) the Digital Asset Service Provider's name and address;
(b) whether the Digital Asset Service Provider executed the Transaction as principal or agent;
(c) the Client's name, account number or other identifier;
(d) a description of the Digital Asset;
(e) whether the Transaction is a sale or purchase;
(f) the price or unit price at which the Transaction was executed;
(g) if applicable, a statement that the Transaction was executed on an execution-only basis;
(h) the date and time of the Transaction;
(i) the total amount payable and the date on which it is due;
(j) the amount of the Digital Asset Service Provider charges in connection with the Transaction, including Commission charges and the amount of any Mark-up or Mark-down, Fees, taxes or duties;
(k) the amount or basis of any charges shared with another Person or statement that this will be made available on request; and
(2) A Digital Asset Service Provider may combine items (f) and (j) above in respect of a Transaction where the Client has requested a note showing a single price combining both of these items.

3.9.2. Appropriateness test

A Digital Asset Service Provider must not carry on a Regulated Activity with or for a Retail Client, who is a non-resident of the Republic of Kazakhstan, unless the Digital Asset Service Provider has carried out an appropriateness test of the Person and formed a reasonable view that the Person has:
(a) adequate skills and expertise to understand the risks involved in trading in Digital Assets or Digital Asset Derivatives (as the case may be); and
(b) the ability to absorb potentially significant losses resulting from trading in Digital Assets or Digital Asset Derivatives (as the case may be).

Guidance:
(1) To form a reasonable view referred to in DAA 3.9.2. in relation to a Person, a Digital Asset Service Provider should consider issues such as whether the Person:

(a) has sufficient knowledge and experience relating to the type of a Digital Asset or Digital Asset Derivative offered, having regard to such factors as:
(i) how often and in what volumes that Person has traded in the relevant type of a Digital Asset or Digital Asset Derivative; and
(ii) the Person's relevant qualifications, profession or former profession;
(b) understands the characteristics and risks relating to Digital Assets or Digital Asset Derivatives, and the volatility of their prices;
(c) understands the impact of leverage, due to which, there is potential to make significant losses in trading in Digital Assets or Digital Asset Derivatives; and
(d) has the ability, particularly in terms of net assets and liquidity available to the Person, to absorb and manage any losses that may result from trading in the Digital Assets or Digital Asset Derivatives offered.
(2) To be able to demonstrate to the AFSA that it complies with DAA 3.9.2., a Digital Asset Service Provider should have in place systems and controls that include:
(a) pre-determined and clear criteria against which a Retail Client's ability to trade in Digital Assets or Digital Asset Derivatives can be assessed;
(b) adequate records to demonstrate that the Digital Asset Service Provider has undertaken the appropriateness test for each Retail Client; and
(c) in the case of an existing Retail Client with whom the Digital Asset Service Provider has previously traded in Digital Assets or Digital Asset Derivatives, procedures to undertake a fresh appropriateness test if:
(i) a new Digital Asset or Digital Asset Derivative with a materially different risk profile is offered to the Retail Client; or
(ii) there has been a material change in the Retail Client's circumstances.
(3) If a Digital Asset Trading Facility Operator forms the view that it is not appropriate for a Person to trade in Digital Assets or Digital Asset Derivatives, the Digital Asset Trading Facility Operator should refrain from offering that service to the Person. As a matter of good practice, the Digital Asset Trading Facility Operator should inform the Person of its decision.

3.10. Provision of key features document and disclosure of risks

3.10.1. Provision of key features document to Person

(1) An Authorised Firm which carries on any one or more of the following Regulated Activities in relation to Digital Assets:

(a) Dealing in Investments as Principal;
(b) Dealing in Investments as Agent;
(c) Managing Investments;
(d) Managing a Collective Investment Scheme;
(e) Providing Custody;
(f) Arranging Custody;
(g) Advising on Investments; and
(h) Arranging Deals in Investments.

must not provide that service or services to a Person unless it has provided the Person with a key features document.
(2) The key features document must contain the following information:
(a) risks associated with and essential characteristics of the Issuer (or another Person responsible for discharging the obligations associated with the rights conferred), and guarantor if any, of the Digital Asset, including their assets, liabilities and financial position;
(b) risks associated with and essential characteristics of the Digital Asset, including the rights and obligations conferred and the type and types of Investments which it constitutes;
(c) whether the Digital Asset is or will be admitted to trading and if so, the details relating to the admission, including details of the facility and whether the facility is within the AIFC;
(d) whether the Client can directly access the trading facility, or whether access is only through an intermediary, and the process for accessing the facility;
(e) risks associated with the use of DLT, in particular those relating to Digital wallets and the susceptibility of private cryptographic keys to misappropriation;
(f) whether the Client, the Authorised Firm or a third party is responsible for providing a Digital wallet service in respect of the Digital Asset, and any related risks (including at whose risk the Client's Digital Assets are held in the Digital wallet, whether it is accessible online or stored offline, what happens if keys to the Digital wallet are lost and what procedures can be followed in such an event);

(g) how the Client may exercise any rights conferred by the Digital Assets such as voting or participation in shareholder actions; and
(h) any other information relevant to the particular Digital Asset which would reasonably assist the Client to understand the product and technology better and to make informed decisions in respect of it.
(3) The key features document must be provided in good time before the relevant service is provided to the Person, to enable that Person to make an informed decision about whether to use the relevant service.
(4) The key features document does not need to be provided to a Person to whom the Authorised Firm has previously provided that information, if there has been no significant change since the information was previously provided.
(5) An Authorised Firm may use a key features document prepared by another Person if it has taken reasonable steps to ensure that the information in that document is complete, accurate and up to date.
(6) If an Authorised Firm provides a Person with a key features document prepared by another Person, the Authorised Firm remains legally accountable to the Person to whom it is provided for the content of the document.

3.10.2. Risk warnings
(1) An Authorised Firm must display prominently on its website the following risk warnings relating to Digital Assets:
(a) that Digital Assets are not legal tender or backed by a government;
(b) that Digital Assets are subject to extreme volatility and the value of the Digital Asset can fall as quickly as it can rise;
(c) that an investor in Digital Assets may lose all, or part, of their money;
(d) that Digital Assets may not always be liquid or transferable;
(e) that investments in Digital Assets may be complex making it hard to understand the risks with buying, selling, holding or lending them;
(f) that Digital Assets can be stolen because of cyber attacks;
(g) that trading in Digital Assets is susceptible to irrational market forces;
(h) that the nature of Digital Assets may lead to an increased risk of Financial Crime;
(i) there being limited or, in some cases, no mechanisms for the recovery of lost or stolen Digital Assets;
(j) the risks of Digital Assets with regard to anonymity, irreversibility of transactions, accidental transactions, transaction recording, and settlement;
(k) that the nature of Digital Assets means that technological difficulties experienced by the Authorised Firm may prevent the access or use of a Client's Digital Assets; and
(l) that investing in, and holding, Digital Assets is not comparable to investing in traditional investments such as Securities.
(2) Where a Digital Asset Service Provider presents any marketing or educational materials and other communications relating to a Digital Asset on a website, in the general media or as part of a distribution made to existing or potential new Clients, it must include the risk warning referred to in (1) in a prominent place at or near the top of each page of the materials or communication.
(3) If the material referred to in (1) is provided on a website or an application that can be downloaded to a mobile device, the warning must be:
(a) statically fixed and visible at the top of the screen even when a person scrolls up or down the webpage; and
(b) included on each linked webpage on the website.

3.10.3. Past performance and forecasts of Digital Assets
(1) A Digital Asset Service Provider must ensure that any information or representation relating to past performance, or any future forecast based on past performance or other assumptions, which is provided to or targeted at Retail Clients:
(a) presents a fair and balanced view of the financial products or financial services to which the information or representation relates;
(b) identifies, in an easy-to-understand manner, the source of information from which the past performance is derived and any key facts and assumptions used in that context are drawn; and
(c) contains a prominent warning that past performance is not necessarily a reliable indicator of future results.
(2) A Digital Asset Service Provider should in providing information about the past performance of a Digital Asset:
(a) consider the knowledge and sophistication of the audience to whom the information is targeted;

(b) fully disclose the source and the nature of the past performance presented;
(c) ensure that the time period used is not an inappropriately short period, or a selective period, that is chosen to show a better performance; and
(d) if a comparison is being made with the same calculation method and period is being used.

3.11. Reconciliation

(1) A Digital Asset Service Provider must:
(a) at least every 25 business days, reconcile its records of Client Accounts held with Third Party Agents with monthly statements received from those Third Party Agents;
(b) at least every six months, count all Safe Custody Digital Assets physically held by the Authorised Firm, or its Nominee Company, and reconcile the result of that count to the records of the Authorised Firm; and
(c) at least every six months, reconcile individual Client ledger balances with the Authorised Firm's records of Safe Custody Digital Asset balances held in Client Accounts.
(2) An Authorised Firm must ensure that the process of reconciliation does not give rise to a conflict of interest.
(3) The Authorised Firm must notify the AFSA where there have been material discrepancies with the reconciliation which have not been rectified.

Guidance

(1) An Authorised firm should maintain a clear separation of duties to ensure that an Employee with responsibility for operating Client Accounts, or an Employee that has authority over Safe Custody Digital Assets, should not perform the reconciliations under DAA 3.11.
(2) Reconciliation performed in accordance with DAA 3.11. must be reviewed by a member of the Authorised Firm who has adequate seniority.
(3) The individual referred to in (2) must provide a written statement confirming that the reconciliation has been undertaken in accordance with the requirements of this section.
(4) A material discrepancy includes discrepancies which have the cumulative effect of being material, such as longstanding discrepancies.

3.12. Clients

3.12.1. Investment limits

A Digital Asset Service Provider must maintain effective systems and controls to ensure compliance with the requirements and limits imposed by the Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC when dealing with a Retail Client who is a resident of the Republic of Kazakhstan.

3.12.2. Calculation of an individual Client's net assets

(1) For the purposes of calculating an individual Client's net assets to treat him as an Assessed Professional Client under Rule 2.5.1(a) of the COB, the Digital Asset Service Provider:
(a) must exclude the value of the primary residence of the Client;
(b) must exclude Digital Assets belonging to the Client that are not on the List of Digital Assets admitted to trading;
(c) must include only 30% of the market value of a Digital Asset admitted to trading, which belongs to the Client, but must include 100% of the market value of a Fiat stablecoin and Commodity stablecoin, which belongs to the Client; and
(e) may include any other assets held directly or indirectly by that Client.

3.13. Prohibitions

(1) A Representative Office must not market a Digital Asset or a Financial Service related to a Digital Asset.
(2) An Authorised Crowdfunding Platform Operating an Investment Crowdfunding Platform must not facilitate a Person investing in the Digital Assets.
(3) An Authorised Firm may not carry on an activity related to a Utility Token or Non-Fungible Token.

(4) The prohibition in (3) does not apply to a Digital Asset Service Provider:
(a) which is authorised to Provide Custody; and
(b) to the extent that it Provides Custody in relation to a Utility Token or Non-fungible Token.

3.14. Obligations

3.14.1. Obligation to report to the AFSA

(1) A Digital Asset Service Provider must submit on a quarterly basis report that should include a financial statement, income statement and calculation of the relevant capital resources and its compliance with these Rules.
(2) The AFSA may request a Digital Asset Service Provider to submit other returns. The list of returns required to be submitted and returns templates may be prescribed by the AFSA from time to time.
(3) Returns submitted to the AFSA must be signed by two (2) Approved Individuals and one of them must be approved to exercise the Finance Officer function.

3.14.2. Obligation to notify the AFSA

If a Digital Asset Service Provider becomes aware, or has a reasonable ground to believe, that it is or may be (or may be about to be) in breach of any of these Rules, that applies to it, it must:
(a) notify the AFSA in writing about the breach and the relevant circumstances immediately and not later than within 1 business day; and
(b) not make any cash transfers or payments or transfers of liquid assets to its Affiliates or Related Persons, whether by way of dividends or otherwise, without the AFSA's written consent.

Guidance:
In dealing with a breach, or possible breach, of this part, the AFSA's primary concern will be the interests of existing and prospective Clients and potential adverse impact on market participants as well as market stability. The AFSA recognises that there will be circumstances in which a problem may be resolved quickly, for example, by support from a parent entity, without jeopardising the interests of Clients and stakeholders. In such circumstances, it will be in the interests of all parties to minimise the disruption to the firm's business. The AFSA's will normally seek to work cooperatively with the Digital Asset Trading Facility Operator in such stressed situations to deal with any problems. There will, however, be circumstances in which it is necessary to take regulatory action to avoid exposing market participants, stakeholders and Clients to the potential adverse consequences of the firm's Failure, and the AFSA will not hesitate to take appropriate action if it considers this necessary.

3.15. AFSA power to impose requirements

Without limiting the powers available to the AFSA under Part 8 of the Framework Regulations, the AFSA may direct an Authorised Market Institution to do or not do specified things that the AFSA considers are necessary or desirable or to ensure the integrity of the AIFC financial markets, including but not limited to directions imposing on a Digital Asset Trading Facility Operator any additional requirements that the AFSA considers appropriate.

Annex 2

FINANCIAL SERVCES FRAMEWORK REGULATIONS
In these Regulations, underlining indicates a new text and strikethrough indicates a removed text

39. Exemption for Authorised Market Institutions
(…)
(3) ~~An Authorised Digital Asset Trading Facility is exempt from the General Prohibition in respect of any Regulated Activity:~~ ***[intentionally omitted]***
(a) ~~which is carried on as a part of the Authorised Digital Asset Trading Facility's business as a Digital Asset trading facility; or~~ ***[intentionally omitted]***
(b) ~~which is carried on for the purposes of, or in connection with, the provision by the Authorised Digital Asset Trading Facility of services designed to facilitate the provision of clearing services by another Person.~~ ***[intentionally omitted]***

57. AFSA power to impose requirements on an Authorised Market Institution
Without limiting the powers available to the AFSA under Part 8 (Supervision ~~of Authorised Persons~~), the AFSA may direct an Authorised Market Institution to do or not do specified things that the AFSA considers are necessary or desirable or to ensure the integrity of the AIFC financial markets, including but not limited to directions:
(a) requiring compliance with any duty, requirement, prohibition, obligation or responsibility applicable to an Authorised Market Institution; or
(b) requiring an Authorised Market Institution to act in a specified manner in relation to a transaction conducted on or through the facilities operated by an Authorised Market Institution, or in relation to a specified class of transactions; or
(c) requiring an Authorised Market Institution to act in a specified manner or to exercise its powers under any rules that the Authorised Market Institution has made.~~; or~~
(d)~~ excluding the application of any requirements for engaging in the activity of Operating a Digital Asset Business imposed by the Rules; or~~ ***[intentionally omitted]***
(e)~~ imposing on an Authorised Person engaged in the activity of Operating a Digital Asset Business any additional requirements that the AFSA considers appropriate.~~ ***[intentionally omitted]***

GENERAL RULES
In these Rules, underlining indicates a new text and strikethrough indicates a removed text

1.2. Authorised Market Institutions
Guidance: Definition of Market Activity
Market Activity is defined in ~~the~~ section 18 of the Framework Regulations as:
(a) Operating an Exchange;
(b) Operating a Clearing House;
(c) ~~Operating a Digital Asset Trading Facility;~~ ***[intentionally omitted]***
(d) Operating a Loan Crowdfunding Platform;
(e) Operating an Investment Crowdfunding Platform~~.~~;
(f) Operating a Private Financing Platform.
(…)

1.2.6. Effective supervision
In assessing whether an applicant is capable of being effectively supervised by the AFSA for the purposes of section 37(1)(c) of the Framework Regulations, the AFSA will consider:
(a) the nature, including the complexity, of the Market Activities that the applicant will carry on;
(b) if the applicant seeks a licence to carry on the Market Activity of Operating an Exchange, ~~a Digital Asset Trading Facility,~~ a Loan Crowdfunding Platform or an Investment Crowdfunding Platform, the size, nature and complexity of any markets in respect of which the applicant will offer its facilities in carrying on that Market Activity;
(…)

1.2.7. Compliance arrangements
(…)
(c) effective arrangements for monitoring and enforcing compliance of its Members with its own rules and, if relevant, its clearing and settlement arrangements; and
(d) if the applicant seeks a licence to carry on the Market Activity of Operating an Exchange, effective arrangements to verify that issuers admitted to trading on its facilities comply with the Market Rules~~.~~; ~~and~~
~~(e) if the applicant seeks a licence to carry on the Market Activity of Operating a Digital Asset Trading Facility, effective arrangements to verify that members admitted to trading on its facilities comply with the Conduct of Business Rules and the Authorised Market Institution Rules.~~
(…)

GENERAL RULES. SCHEDULE 1: REGULATED ACTIVITIES
30. Operating a Digital Asset Trading Facility
Operating a Digital Asset Trading Facility means operating a facility which functions regularly and brings together multiple parties (whether as principal or agent) with a view to the entering into of contracts:
(a) to buy, sell or exchange Digital Assets for a Fiat currency; and/or
(b) to exchange one Digital Asset for another Digital Asset, in its Facility, in accordance with its non-discretionary rules~~.~~; and/or
(c) to buy, sell or exchange Digital Assets for a commodity.

GENERAL RULES. SCHEDULE 4: MARKET ACTIVITIES
Schedule 4: Market Activities.
(…)
3. ~~Operating a Digital Asset Trading Facility~~
~~Operating a Digital Asset Trading Facility means operating a facility which functions regularly and brings together multiple parties (whether as principal or agent) with a view to the entering into of contracts:~~
~~(a) to buy, sell or exchange Digital Assets for a Fiat currency; and/or~~
~~(b) to exchange one Digital Asset for another Digital Asset, in its Facility, in accordance with its non-discretionary rules.~~ ***[intentionally omitted]***

GLOSSARY

In these Rules, underlining indicates a new text and strikethrough indicates a removed text

GLOSSARY. 1. Application. (t) AIFC Rules on Regulation of Digital Asset Activities (DAA).
(…)

Algorithmic stablecoin	A Digital Asset which uses, or purports to use, an algorithm to increase or decrease the supply of Digital Assets in order to stabilise its price or reduce volatility in its price
~~Authorised Private~~ Digital Asset Trading Facility Operator	A Centre Participant which has been licensed by the AFSA to carry on the Regulated ~~Market~~ Activity of Operating a Digital Asset Trading Facility.
Client Account	In relation to Client Investments or Client Digital Assets is an account which: (a) is held with a Third Party Agent or by an Authorised Firm which is authorised under its Licence to Provide Custody; (b) is established to hold Client Assets; (c) when held by a Third Party Agent, is maintained in the name of: (i) if a Domestic Firm, the Authorised Firm; or (ii) if not a Domestic Firm, a Nominee Company controlled by the Authorised Firm; and (d) includes the words 'Client Account' in its title.
Commodity stablecoin	A Digital Asset whose value purports to be determined by reference to a commodity (e.g., gold, oil).
Digital Asset Business	Any one or more of the following Regulated Activities in relation to Digital Assets: Dealing in Investments as Principal; Dealing in Investments as Agent; Managing Investments; Managing a Collective Investment Scheme;) Providing Custody; Arranging Custody; Advising on Investments; Arranging Deals in Investments; Providing Money Services; and Operating a Digital Asset Trading Facility. A Person wishing to carry on or more of the above Regulated Activities in relation to Digital Assets, cannot carry on the Regulated Activities in relation to other types of Investments.
Digital Asset Derivative	A Derivative the value of which is determined by reference to: a Digital Asset; or an index that includes a Digital Asset.
DASP	Digital Asset Service Provider
Digital Asset Service Provider	A Centre Participant which has been licensed by the AFSA to carry on one or more of the following Regulated Activities in relation to Digital Assets: Operating a Digital Asset Trading Facility; Dealing in Investments as Principal; Dealing in Investments as Agent; Managing Investments; Providing Custody; Arranging Custody; Advising on Investments; Arranging Deals in Investments; and Providing Money Services.

	A Person wishing to carry on one or more of the above Regulated Activities in relation to Digital Assets, cannot carry on the Regulated Activities in relation to other types of Investments.
Digital Asset Custodian	Authorised Firm which carries on the Regulated Activity of Providing Custody in relation to Digital Assets.
DATF	Digital Asset Trading Facility
Digital Asset Trading Facility	A facility on which Digital Assets, rights or interests in Digital Assets are traded.
Digital Asset Trading Facility Operator	A Centre Participant which is licensed by the AFSA to carry on the Regulated Activity of Operating a Digital Asset Trading Facility.
Digital Asset (or Private Electronic Currency or Private E-money)	A digital representation of value that (1) can be digitally traded and functions as (a) a medium of exchange; or (b) a unit of account; or (c) a store of value; (2) can be exchanged back-and-forth for Fiat Currency, but is neither issued nor guaranteed by the government of any jurisdiction, and (3) fulfils the above functions only by agreement within the community of users of the Digital Asset; and accordingly (4) is to be distinguished from Fiat Currency and E-money. An Excluded Digital Asset is excluded from the scope of the DAA.
Digital wallet Service Provider	An Authorised Firm Providing Custody of Digital Assets by holding and controlling the public and private cryptographic keys relating to the Digital Assets.
Direct Electronic Access	Direct Electronic Access means: (a) an arrangement (called direct market access), through which a Member or a client of a member is able to electronically transmit, using the Member's trading code, an order relating to a Digital Asset, Security, Unit in a Listed Fund or Qualified Investment directly to the facility operated by the Authorised Market Institution, Digital Asset Trading Facility Operator or MTF or OTF Operator. It includes arrangements for the use, by a Person, of the infrastructure (or connecting system) of the Member, client of the Member or another participant; or (b) an arrangement (called sponsored access) through which a Member or a client of a member is able to electronically transmit, using the Member's trading code, an order to the facility operated by the Authorised Market Institution or MTF or OTF Operator without using the infrastructure (or connecting system) of the Member or another participant or client.
Distributed Ledger Technology	A class of technologies that support the recording of encrypted data where the data: (a) is held on a distributed ledger; (b) is electronically accessible, from multiple locations, by a network of participants; and (c) can be updated by those participants, based on agreed consensus, protocol or procedures.
DLT	Distributed Ledger Technology
Domestic Firm	An Authorised Person or Ancillary Service Provider which: (a) has its registered and head office in the AIFC; or (b) if it is a subsidiary of an Undertaking whose principal place of business and head office is in a jurisdiction other than the AIFC, has its registered office in the AIFC.
Excluded Digital Asset	A Digital Asset which is: (a) a Non-Fungible Token; (b) a Utility Token; or (c) a digital currency issued by any government, government agency, central bank, or another monetary authority.
Execute or Execution	The exercise of a Client order that results in a binding transaction.

Fiat stablecoin	A Digital Asset whose value purports to be determined by reference to a Fiat Currency or a basket of Fiat Currencies.
Investment Business	The business of: (a) Dealing in Investments as Principal; (b) Dealing in Investments as Agent; (c) Managing Investments; (d) Managing a Collective Investment Scheme; (e) Providing Custody; (f) Arranging Custody; (g) Acting as the Trustee of a Fund; (h) Advising on Investments; (i) Arranging Deals in Investments; (j) Managing a Restricted Profit Sharing Investment Account; or (k) Operating an Exchange. but not including Digital Asset Business.
List of Digital Assets admitted to trading	A list of Digital Assets which could be traded in the AIFC and do not require the AFSA's approval.
Member	A Person who is entitled, under an arrangement between him and an Authorised Market Institution, a Digital Asset Trading Facility Operator, a MTF Operator or an OTF Operator, to use that institution's or operator's facilities
Non-Fungible Token	An Investment which: (a) is unique and not fungible with any other Non-Fungible Token; (b) related to an identified asset; and (c) is used to prove the ownership or provenance of the asset.
Operating a Digital Asset Trading Facility	The Regulated ~~Market~~ Activity defined in paragraph 30~~3~~ of Schedule 1~~4~~ of the AIFC General Rules.
Privacy Device	Any technology, Digital wallet or another mechanism or device (excluding a VPN), which has any feature or features used, or intended to be used, to hide, anonymise, obscure or prevent the tracing of any of the following information: (a) a Digital Asset transaction; or (b) the identity of the holder of a Digital Asset; or (c) the cryptographic key associated with a Person; or (d) the identity of parties to a Digital Asset transaction; or (e) the value of a Digital Asset transaction; or (f) the beneficial owner of a Digital Asset.
Privacy Token	A Digital Asset where the Digital Asset or the DLT or another similar technology used for the Digital Asset, has any feature or features that are used, or intended to be used, to hide, anonymise, obscure or prevent the tracing of any of the following information: (a) a Digital Asset transaction; or (b) the identity of the holder of a Digital Asset; or (c) the cryptographic key associated with a Person; or (d) the identity of parties to a Digital Asset transaction; or (e) the value of a Digital Asset transaction; or (f) the beneficial owner of a Digital Asset.
Safe Custody Digital Assets	Digital Assets held or to be held for safekeeping by an Authorised Firm or Third Party Agent.
Security Token	A Digital Asset that represents ownership of a Security.
Self-Custody of Digital Assets	The holding and controlling of Digital Assets by their owner, through the owner holding and controlling the public and private cryptographic keys relating to the Digital Assets.
Self-hosted Digital Wallet	A software or hardware that enables a person to store and transfer Digital Assets on his own behalf, and in relation to which the public and private cryptographic keys are controlled or held by that Person.

Third Party Agent	In relation to a Client Account, means an Authorised Firm or Regulated Financial Institution (including a bank, custodian, an intermediate broker, a settlement agent, a clearing house, an exchange and 'over the counter' counterparty) that is a separate legal entity from the Authorised Firm that is required under COB to establish the Client Account.
Third Party Digital wallet Service Provider	(1) A Digital wallet Service Provider other than a Digital Asset Trading Facility Operator Providing Custody of Digital Assets traded on its facility; or (2) A Person in another jurisdiction Providing Custody of Digital Assets by holding and controlling the public and private cryptographic keys relating to the Digital Assets, which is authorized and appropriately supervised for that activity by a Financial Services Regulator.
Travel Rule	Has the meaning given to it in FATF's *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers* [October 2021], as may be amended from time to time
Utility Token	A Digital Asset: (a) which can be used by the holder only to pay for, receive a discount on, or access a product or service (whether current or proposed); and (b) the product or service referred to in (a) is provided by the issuer of the Digital Asset or of another entity in the issuer's Group.
VPN	A virtual private network that creates a safe, encrypted online connection for internet users.

(…)
Guidance: Purpose and application of AMI

- the licensing requirements, or standards, which an applicant must satisfy to be granted a Licence to carry on either of the Market Activities of Operating an Investment Exchange~~, Operating Digital Assets Trading Facility~~ and Operating a Clearing House;
(…)
- ~~Chapter 6 contains additional rules and guidance applicable to Authorised Digital Assets Trading Facility.~~
(…)

1. INTRODUCTION
1.1. Introduction
1.1.1. Definitions
(1) An Authorised Market Institution is a Centre Participant which has been licensed by the AFSA to carry on one or more Market Activities. An Authorised Market Institution can be an Authorised Investment Exchange, ~~an Authorised Digital Asset Trading Facility,~~ an Authorised Clearing House and/or an Authorised Crowdfunding Platform.
(7) ~~An Authorised Digital Asset Trading Facility is a Centre Participant which has been licensed by the AFSA to carry on the Market Activity of Operating a Digital Asset Trading Facility.~~***[intentionally omitted]***
(…)

2.4.4. Resources of Members
(…)
(2) The requirements in (1) do not apply to~~:~~
(a) ~~an~~ an Authorised Crowdfunding Platform (or its Clients)~~;~~.~~ or~~
~~(b) the Member of an Authorised Digital Asset Trading Facility if the Member is a body corporate or an individual (natural person) that carries on the activity solely as principal~~. ***[intentionally omitted]***
(…)

2.4.7. Testing relating to Members' technology systems
(…)
(4) The requirements in (1)-(3) do not apply to~~:~~
(a) an Authorised Crowdfunding Platform (or its Clients)~~;~~.~~ or~~
~~(b) the Member of an Authorised Digital Asset Trading Facility if the Member is a body corporate or an individual (natural person) that carries on the activity solely as principal~~.

2.5. Business Rules
2.5.1. Requirement to prepare Business Rules
(…)
(d) Admission to Trading Rules, prepared in accordance with AMI 3.2 ~~or AMI 6.3~~, or Admission to Clearing Rules, prepared in accordance with AMI 4.1, governing the admission of Securities~~,~~ or Units in a Listed Fund ~~or Digital Assets~~ to trading, or clearing and settlement, as appropriate to its facilities;
(e) Listing Rules, prepared in accordance with AMI 3.6, setting out the rules and conditions applicable to a Person who wishes to have Securities or Units in a Listed Fund included in an Official List; and

(f) any other matters necessary for the proper functioning of the Authorised Market Institution and the facilities operated by it.
~~The requirements in (c) and (e) do not apply to the Authorised Digital Asset Trading Facility.~~

2.6. Membership
2.6.1. Persons eligible for Membership
(1) An Authorised Market Institution~~, except an Authorised Digital Asset Trading Facility,~~ may only admit as a Member a Person who satisfies admission criteria set out in its Membership Rules and who is either:
(a) an Authorised Firm whose Licence permits it to carry on the Regulated Activities of Dealing in Investments; or
(b) a Recognised Non-AIFC Member.
~~(2) An Authorised Digital Asset Trading Facility may only admit as a Member a Person who satisfies admission criteria set out in its Membership Rules and which is:~~ ***[intentionally omitted]***
~~(a) an Authorised Firm whose Licence permits it to carry on the Regulated Activities of Dealing in Investments;~~ ***[intentionally omitted]***
~~(b) a Recognised Non-AIFC Member; or~~ ***[intentionally omitted]***
~~(c) a body corporate or an individual (natural person) which carries on the activity solely as principal.~~ ***[intentionally omitted]***

2.7. Direct Electronic Access
2.7.1. Direct Electronic Access
Direct Electronic Access means any arrangement, such as the use of the Member's trading code, through which a Member or the clients of that Member are able to transmit electronically orders relating to Securities~~,~~ or Units in a Listed Fund ~~or Digital Asset~~ directly to the facility provided by the Authorised Market Institution~~ and includes arrangements which involve the use by a Person of the infrastructure of the Authorised Digital Asset Trading Facility or the Member or participant or client or any connecting system provided by the Authorised Digital Asset Trading Facility or Member or participant or client, to transmit the orders and arrangements where such an infrastructure is not used by a Person~~.
(…)

2.9.2. Custody and investment risk
(1) An Authorised Market Institution must have effective means to address risks relating to:
(a) custody of its own assets, in accordance with (2), if it is an Authorised Clearing House; or
(b) investments, in accordance with (3), if it is an Authorised Investment Exchange.~~; or~~
(c)~~ Digital Assets, if it is an Authorised Digital Asset Trading Facility.~~ ***[intentionally omitted]***
(…)
~~**6. RULES APPLICABLE TO AN AUTHORISED DIGITAL ASSET TRADING FACILITY**~~
~~**6.1. Main requirements relating to trading on the facility**~~
~~(1) An Authorised Digital Asset Trading Facility must, at the time a Licence is granted and at all times thereafter, have:~~
~~(a) transparent and non-discriminatory rules and procedures to ensure fair and orderly trading of Digital Assets on its facility;~~
~~(b) objective criteria governing access to its facility;~~
~~(c) objective and transparent criteria for determining the Investments that can be traded on its facility; and~~
~~(d) adequate technology resources.~~
~~(2) An Authorised Digital Asset Trading Facility must maintain effective arrangements to verify that its members comply with requirements set out in COB, AML.~~
~~(3) An Authorised Digital Asset Trading Facility must not introduce a liquidity incentive scheme other scheme for encouraging bids on a trading venue or to increase the volume of business transacted unless it has obtained the prior approval of the AFSA.~~
~~(4) For the purposes of (1), an Authorised Digital Asset Trading Facility must make available to the public, without any charges, data relating to the quality of execution of transactions on the Authorised Digital Asset Trading Facility on at least an annual basis. Reports must include details about price, costs, speed and likelihood of execution for individual Digital Assets.~~

~~6.2. Requirement to prepare Rules~~
~~(1) An Authorised Digital Asset Trading Facility's Rules must:~~
~~(a) be based on objective criteria;~~

(b) be non-discriminatory;
(c) be clear and fair;
(d) be made publicly available free of charge;
(e) contain provisions for the resolution of Members' and other participants' disputes;
(f) contain provisions for penalties or sanctions which may be imposed by the Authorised Digital Asset Trading Facility for a breach of the Rules; and
(g) contain provisions for an appeal process from the decisions of the Authorised Digital Asset Trading Facility.
(2) An Authorised Digital Asset Trading Facility must seek prior approval of its Rules (Business Rules, Admission to Trading Rules, Membership Rules) and of amendments to its Rules by:
(a) making its Rules available for market consultation for no less than 30 days; and
(b) obtaining approval of the AFSA.
(3) Where an Authorised Digital Asset Trading Facility has made any amendments to its Rules, it must have adequate procedures for notifying users and the AFSA of such amendments with a notice period of at least 30 days prior to making any amendments to its Rules available for market consultation.
(4) An Authorised Digital Asset Trading Facility must have procedures in place to ensure that its Rules are monitored and enforced.

6.3. Admission of Digital Assets to trading
6.3.1. Admission to Trading Rules
(1) An Authorised Digital Asset Trading Facility must make clear and transparent rules concerning the admission of Digital Assets to trading on its facilities.
(2) The rules of the Authorised Digital Asset Trading Facility must ensure that:
(a) Digital Assets admitted to trading on an Authorised Digital Asset Trading Facility's facilities are capable of being traded in a fair, orderly and efficient manner; and
(b) Digital Assets admitted to trading on an Authorised Digital Asset Trading Facility's facilities are freely negotiable.

6.3.2. Application for admission of Digital Assets to Trading
(1) Applications for the admission of a Digital Asset to trading can be made to an Authorised Digital Asset Trading Facility by the issuer of the Digital Asset, by a third party on behalf of and with the consent of the issuer of the Digital Asset, or by a Member of an Authorised Digital Asset Trading Facility.
(2) A Digital Asset can also be admitted to trading on the Authorised Digital Asset Trading Facility's own initiative.
(3) An Authorised Digital Asset Trading Facility must, before admitting any Digital Asset to trading:
(a) be satisfied that the applicable requirements, including those in its Admission to Trading Rules, have been or will be fully complied with in respect of such Digital Asset and
(b) obtain approval of the AFSA in respect of such Digital Asset.
(4) For the purposes of (1), an Authorised Digital Asset Trading Facility must notify an applicant in writing of its decision in relation to the application for admission of the Digital Asset to trading. In the case that such decision is to deny the application, the written notice should indicate (i) whether the application has been considered by the AFSA, and if so, (ii) the AFSA's determination in respect thereof.
(5) For purposes of 3(b), an application to AFSA by Authorised Digital Asset Trading Facility shall include:
(a) a copy of the admission application; and
(b) any other information requested by the AFSA.

6.3.3. Decision-making procedures for the AFSA in relation to applications for approval of the admission of Digital Assets to trading
(1) Where an Authorised Person Operating a Digital Asset Trading Facility applies for approval of the admission of a Digital Asset to trading, the AFSA may:
(a) approve the application;
(b) deny the application; or
(c) approve the application subject to conditions or restrictions.
(2) The AFSA may exercise its powers under (1)(b) where the AFSA reasonably considers that:

(a) granting the Digital Assets admission to trading of Digital Assets would be detrimental to the interests of Persons dealing in the relevant Digital Assets using the facilities of an Authorised Person Operating a Digital Asset Trading Facility or otherwise; or
(b) any requirements imposed by the AFSA or in the Rules of an Authorised Digital Asset Trading Facility as are applicable have not been or will not be complied with; or
(c) the Issuer of the Digital Assets has failed or will fail to comply with any obligations applying to it including those relating to having its Digital Assets admitted to trading or traded in another jurisdiction.
(3) Where the AFSA denies an application for approval of admission of a Digital Asset to trading pursuant to (2), such Digital Assets must not be admitted by an Authorised Person Operating a Digital Asset Trading Facility to its facility.
(4) Where the AFSA approves an application for approval of admission of a Digital Asset to trading subject to conditions or restrictions, the Authorised Person Operating a Digital Asset Trading Facility is responsible for implanting such conditions and restrictions in admitting the Digital Asset to trading, and such conditions or restrictions may not be varied or removed without the approval of the AFSA.

6.3.4. Undertaking to comply with the acting law of the AIFC
An Authorised Digital Asset Trading Facility may not admit Digital Asset to trading unless the person who seeks to have Digital Assets admitted to trading:
(a) gives an enforceable undertaking to the AFSA to submit unconditionally to the jurisdiction of the AIFC in relation to any matters which arise out of or which relate to its use of the facilities of the Authorised Market Institution;
(b) agrees in writing to submit unconditionally to the jurisdiction of the AIFC Courts in relation to any disputes, or other proceedings in the AIFC, which arise out of or relate to its use of the facilities of the Authorised Market Institution; and
(c) agrees in writing to subject itself to the acting law of the AIFC in relation to its use of the facilities of the Authorised Market Institution.

6.3.5. Review of compliance
The Authorised Digital Asset Trading Facility must maintain arrangements regularly to review whether the Digital Assets admitted to trading on its facilities comply with the Admission to Trading Rules.

6.4. Suspending or removing Digital Assets from trading
6.4.1. Power to suspend
(1) The rules of an Authorised Digital Asset Trading Facility must provide that the Authorised Digital Asset Trading Facility have the power to suspend or remove from trading on its facilities any Digital Assets with immediate effect or from such date and time as may be specified where it is satisfied that there are circumstances that warrant such action or it is in the interests of the AIFC.
(2) The AFSA may direct an Authorised Person Operating a Digital Asset Trading Facility to suspend or remove Digital Assets from trading with immediate effect or from such date and time as may be specified if it is satisfied there are circumstances that warrant such action or it is in the interests of the AIFC.
(3) The AFSA may withdraw a direction made under (2) at any time.
(4) Digital Assets that are suspended from trading of Digital Assets remain admitted to trading for the purposes of this Chapter.
(5) The AFSA may prescribe any additional requirements or procedures relating to the removal or suspension of Digital Assets from or restoration of Digital Assets to trading.

6.4.2. Limitation on power to suspend or remove Digital Assets from trading
The rules of an Authorised Digital Asset Trading Facility must contain provisions for orderly suspension and removal from trading on its facilities any Digital Asset which no longer complies with its rules taking into account the interests of investors and the orderly functioning of the financial markets of the AIFC.

6.4.3. Publication of decision
(1) Where the Authorised Digital Asset Trading Facility suspends or removes any Digital Asset from trading on its facilities, it must notify the AFSA in advance and make that decision public by issuing a public notice on its website.
(2) Where the Authorised Digital Asset Trading Facility lifts a suspension or re-admits any Digital Asset to trading on its facilities, it must notify the AFSA in advance and make that decision public by issuing a public notice on its website.

(3) Where an Authorised Digital Asset Trading Facility has made any decisions on admission, suspension, or removal of Digital Assets from trading on its facilities, it must have adequate procedures for notifying users of such decisions.

6.5. Transparency obligations

6.5.1. Trading transparency obligation

An Authorised Digital Asset Trading Facility must make available to the public:

(a) the current bid and offer prices of Digital Assets traded on its systems on a continuous basis during normal trading hours;

(b) the price, volume and time of the transactions executed in respect of Digital Assets traded on its facilities in as close to real-time as technically possible; and

(c) provide price, volume, time and counterparty details to the AFSA within 24 hours of the close of each trading day via a secure electronic feed.

6.5.2. Public notice of suspended or terminated Membership

The Authorised Digital Asset Trading Facility must promptly issue a public notice on its website in respect of any Member that has a Licence to carry on Market Activities or Regulated Activities whose Membership is suspended or terminated.

6.5.3. Cooperation with office-holder

The Authorised Digital Asset Trading Facility must cooperate, by the sharing of information and otherwise, with the AFSA, any relevant office-holder and any other authority or body having responsibility for any matter arising out of, or connected with, the default of a Member of the Digital Asset Trading Facility.

6.6. Additional requirements on technology resources

6.6.1. Cyber-security policy

(1) An Authorised Digital Asset Trading Facility shall implement a written cyber security policy setting forth its policies and procedures for the protection of its electronic systems and members and counterparty data stored on those systems, which shall be reviewed and approved by the Authorised Digital Asset Trading Facility's governing body at least annually.

(2) The cyber security policy must, as a minimum, address the following areas:

(a) information security;

(b) data governance and classification;

(c) access controls;

(d) business continuity and disaster recovery planning and resources;

(e) capacity and performance planning;

(f) systems operations and availability concerns;

(g) systems and network security;

(h) systems and application development and quality assurance;

(i) physical security and environmental controls;

(j) customer data privacy;

(k) vendor and third-party service provider management; and

(l) incident response.

(3) An Authorised Digital Asset Trading Facility must advise the AFSA immediately if it becomes aware, or has reasonable grounds to believe, that a significant breach by any Person of its cyber security policy may have occurred or may be about to occur.

6.6.2. Technology governance

An Authorised Digital Asset Trading Facility must, as a minimum, have in place systems and controls with respect to the procedures describing the creation, management and control of digital wallets and private keys.

6.6.3. Trading controls

An Authorised Digital Asset Trading Facility must be able to:

(a) reject orders that exceed its pre-determined volume and price thresholds, or that are clearly erroneous;

(b) temporarily halt or constrain trading on its facilities if necessary or desirable to maintain an orderly market; and

(c) cancel, vary, or correct any order resulting from an erroneous order entry and/or the malfunctioning of the system of a Member.

6.6.4. Settlement and Clearing facilitation services

(1) An Authorised Digital Asset Trading Facility must ensure that satisfactory arrangements are made for securing the timely discharge (whether by performance, compromise or otherwise), clearing and settlement of the rights and liabilities of the parties to transactions effected on the Authorised Digital Asset Trading Facility (being rights and liabilities in relation to those transactions).

(2) An Authorised Digital Asset Trading Facility acting as a Digital Asset Depository must:

(a) have appropriate rules, procedures, and controls, including robust accounting practices, to safeguard the rights of Digital Assets issuers and holders, prevent the unauthorised creation or deletion of Digital Assets, and conduct periodic and at least daily reconciliation of each Digital Asset balance it maintains for issuers and holders;

(b) prohibit overdrafts and debit balances in Digital Assets accounts;

(c) maintain Digital Assets in an immobilised or dematerialised form for their transfer by book entry;

(d) protect assets against custody risk through appropriate rules and procedures consistent with its legal framework;

(e) ensure segregation between the Digital Asset Depository's own assets and the Digital Assets of its participants and segregation among the Digital Assets of participants; and

(f) identify, measure, monitor, and manage its risks from other custody related activities that it may perform.

6.7. Clients of an Authorised Digital Asset Trading Facility and Investment limits

(1) Members of an Authorised Digital Asset Trading Facility and their clients will be Clients of an Authorised Digital Asset Trading Facility.

(2) An Authorised Digital Asset Trading Facility must maintain effective systems and controls to ensure that a Retail Client using its service does not invest, in respect of all Digital Assets in aggregate calculated over a period of one month, an amount which exceeds the greater of:

(a) USD 1,000; or

(b) the lesser of (i) 10 percent of the annual income; or (ii) 5 percent of the net worth of such Retail Client (excluding the value of the primary residence), up to a maximum aggregate amount of USD100,000.

CONTENTS

1.2.2. Exclusions in relation to certain categories of Centre Participant

For the avoidance of doubt, the requirements in COB do not apply to:

(a) a Representative Office;

(b) an Authorised Market Institution (other than an Authorised Crowdfunding Platform ~~and an Authorised Digital Asset Trading Facility~~), except for COB 3 (Communications with Clients and Financial Promotions); or

(c) an Authorised Crowdfunding Platform, except for COB 3 (Communications with Clients and Financial Promotions), COB 4 (Key Information and Client Agreement), COB 7 (Conflicts of Interest), COB 8 (Client Assets) and COB Schedule 2 (Key Information and Content of Client Agreement~~); or~~

~~(d) an Authorised Digital Asset Trading Facility, except for COB 2 (Client Classification) and COB 3 (Communications with Clients and Financial Promotions)~~.

(…)

~~For the purposes of 1.2.2(d), references in COB 2 and COB 3 to:~~

~~(a) "Authorised Firms" shall be read as if it were a reference to "an Authorised Digital Asset Trading Facility "; and~~

~~(b) "Regulated Activities" shall be read as if it were a reference to "Market Activities".~~

(…)

~~**17. OPERATORS OF A DIGITAL ASSET BUSINESS**~~

~~**17.1. Application**~~

~~This chapter applies to an Authorised Person engaged in the activity of Operating a Digital Asset Business.~~

~~**Guidance**~~

~~The following activities do not constitute Operating a Digital Asset Business:~~

~~trading of Digital Assets for the Person's own investment purpose;~~

~~the issuance of Digital Assets by a Person and their administration (including sale, redemption);~~

~~any other activity or arrangement that is deemed by the AFSA to not constitute Operating a Digital Asset Business, where necessary and appropriate in order for the AFSA to pursue its objectives.~~

~~**17.2. Rules Applicable to an Authorised Digital Asset Trading Facility**~~ **Operator**

~~In addition to all requirements applicable to Authorised Persons in these rules, GEN, and AML, an Authorised Person carrying on the Market Activity of Operating a Digital Asset Trading Facility must comply with the applicable requirements set out in the AMI, unless the requirements in this chapter expressly provide otherwise.~~

~~**17.3. Admission of Digital Assets to trading**~~

~~An Authorised Person Operating a Digital Asset Trading Facility may grant admission of Digital Assets to trading only where it is satisfied that such admission is in accordance with the AMI and an Authorised Digital Asset Trading Facility's Admission to Trading Rules.~~

~~An Authorised Person Operating a Digital Asset Trading Facility must not permit trading of Digital Assets on its facilities unless those Digital Assets are admitted to, and not suspended from, trading by~~

the Authorised Person Operating a Digital Asset Trading Facility pursuant to Chapter 6 of AMI. ***[intentionally omitted]***

17.4. Additional disclosure requirements

Prior to entering into an initial transaction for, on behalf of, or with a Client, an Authorised Person Operating a Digital Asset Business shall disclose in a clear, fair and not misleading manner:

(a) all terms, conditions and risks relating to the Digital Assets that have been admitted to trading and/or is the subject of the transaction;

(b) all material risks associated with its products, services and activities; and

(c) all details on the amount and the purpose of any premiums, fees, charges or taxes payable by the Client, whether or not these are payable to the Operating a Digital Asset Business. ***[intentionally omitted]***

17.5. The risks to be disclosed pursuant to COB 17.4

The risks to be disclosed pursuant to COB 17.4. include, but are not limited to, the following:

(a) Digital Assets not being legal tender or backed by a government;

(b) the value, or process for valuation, of Digital Assets, including the risk of a Digital Assets having no value;

(c) the volatility and unpredictability of the price of Digital Assets relative to Fiat Currencies;

(d) that trading in Digital Assets is susceptible to irrational market forces;

(e) that the nature of Digital Assets may lead to an increased risk of Financial Crime;

(f) that the nature of Digital Assets may lead to an increased risk of cyber-attack;

(g) there being limited or, in some cases, no mechanism for the recovery of lost or stolen Digital Assets;

(h) the risks of Digital Assets with regard to anonymity, irreversibility of transactions, accidental transactions, transaction recording, and settlement;

(i) that there is no assurance that a Person who accepts a Digital Asset as payment today will continue to do so in the future;

(j) that the nature of Digital Assets means that technological difficulties experienced by the Authorised Person may prevent the access or use of a Client's Digital Assets;

(k) any links to Digital Assets related activity outside the AIFC, which may be unregulated or subject to limited regulation; and

(l) any regulatory changes or actions by the AFSA or Non-AIFC Regulator that may adversely affect the use, transfer, exchange, and value of a Digital Asset. ***[intentionally omitted]***

17.6. Complaints

An Authorised Person Operating a Digital Asset Business shall establish and maintain written policies and procedures to fairly and timely resolve complaints made against it or other parties (including members).

An Authorised Person Operating a Digital Asset Business must provide, in a clear and conspicuous manner: on its website or websites; in all physical locations; and in any other location as the AFSA may prescribe, the following disclosures:

(a) the mailing address, email address, and telephone number for the receipt of complaints;

(b) a statement that the complainant may also bring his or her complaint to the attention of the AFSA;

(c) the AFSA's mailing address, website, and telephone number; and

(d) such other information as the AFSA may require.

An Authorised Person Operating a Digital Asset Business shall report to the AFSA any change in its complaint policies or procedures within ten days.

An Authorised Person Operating a Digital Asset Business must maintain a record of any complaint made against it or other parties (including members) for a minimum period of six years from the date of receipt of the complaint. ***[intentionally omitted]***

17.7. Obligation to report transactions

An Authorised Person Operating a Digital Asset Business shall report to the AFSA details of transactions in Digital Assets traded on its facility which are executed, or reported, through its systems.

The AFSA may, by written notice or Guidance, specify:

(a) the information to be included in reports made under the preceding paragraph; and

(b) the manner in which such reports are to be made. ***[intentionally omitted]***

17.8. AFSA power to impose a prohibition or requirement

~~The AFSA may prohibit an Authorised Person Operating a Digital Asset Business from:~~
~~(a) entering into certain specified transactions or types of transactions; or~~
~~(b) outsourcing any of its functions or activities to a third party.~~
~~The AFSA may, by written notice or guidance, set fees payable by an Authorised Person Operating a Digital Asset Business to the AFSA on certain specified transactions or types of transactions.~~
[intentionally omitted]

SCHEDULE 2: KEY INFORMATION AND CONTENT OF CLIENT AGREEMENT

1.	CORE INFORMATION
(…)	(…)
5.	ADDITIONAL INFORMATION FOR DIGITAL ASSET TRADING FACILITY OPERATORS AND DIGITAL ASSET SERVICE PROVIDERS PROVIDING CUSTODY
	The additional information required where an Authorised Firm Provides Custody in relation to Digital Assets:
	a breakdown of all fees and charges payable for a transfer of Digital Assets (a "transfer") and when they are charged;
	the information required to carry out a transfer;
	the form and procedures for giving consent to a transfer;
	an indication of the time it will normally take to carry out a transfer;
	details of when a transfer will be considered to be complete;
	how, and in what form, information and communications relating to transfer services will be provided to the Client, including the timing and frequency of communications and the language used and technical requirements for the Client's equipment and software to receive the communications;
	clear policies and procedures relating to unauthorised or incorrectly executed transfers, including when the Client is and is not entitled to redress;
	clear policies and procedures relating to situations where the holding or transfer of Digital Assets may have been compromised, such as if there has been hacking, theft or fraud; and
	details of the procedures the Digital Asset will follow to contact the Client if there has been suspected or actual hacking, theft or fraud.

AIFC FEES RULES

In these Rules, underlining indicates a new text and strikethrough indicates a removed text

SCHEDULE 1: APPLICATION FEES PAYABLE TO THE AFSA FOR REGULATED ACTIVITIES

1.1 Application fees for applying for Licence to carry on Regulated Activities

Regulated Activities	Fee (USD)*
Operating a Representative Office	3 000
(…)	(…)
Operating an Organised Trading Facility	5000
Operating a Digital Asset Trading Facility	70 000

(…)

SCHEDULE 2: APPLICATION FEES PAYABLE TO THE AFSA FOR MARKET ACTIVITIES

1.2 Application fees for applying for Licence to carry on Market Activities

Application fee by activities	Fee (USD)
Operator of a Clearing House	125 000
Operator of an Investment Exchange	125 000
~~Operator of a Digital Asset Trading Facility~~	~~70 000~~
Operator of a Crowdfunding Platform	5 000
Operating a Private Financing Platform	5 000

(…)

SCHEDULE 6: ANNUAL SUPERVISION FEES PAYABLE TO THE AFSA

6.1 Annual supervision fees for Regulated Activities

Annual supervision fees for Regulated Activities are determined by the activities the Authorised Firm conducts as set out below:

Regulated Activities	Fee (USD)*
Operating a Representative Office	1 000
(…)	(…)
Operating an Organised Trading Facility	• 3 000 USD (fixed); and • trading levy of 0.0006% of the average daily trading value (variable)**. Note: AFSA will not invoice the trading levy (variable) fee unless it exceeds 500 USD
Operating a Digital Asset Trading Facility	35 000

(…)

6.2 Annual supervision fees for Market Activities

Annual supervision fees for Market Activities are determined by the activities the Authorised Market Institution conducts as set out below:

Application fee by activities	Fee (USD)
Operator of a Clearing House	62 500
Operator of an Investment Exchange	62 500
~~Operator of a Digital Asset Trading Facility~~	~~35 000~~
Operator of a Crowdfunding Platform	3 000
Operating a Private Financing Platform	3 000

(…)

6. CUSTOMER DUE DILIGENCE
6.1. Conducting Customer Due Diligence
6.1.1. Obligation to conduct Customer Due Diligence

A Relevant Person must:
(a) conduct CDD under AML 6.3.1 for each of its customers including when the customer is carrying out occasional transactions the value of which singularly or in several linked operations (whether at the time or later), equal or exceed USD 15,000; and
(a-a) conduct CDD under AML 6.3.1 for each of its customers including when the customer is carrying out occasional transactions with Digital Assets the value of which singularly or in several linked operations (whether at the time or later), equal or exceed USD 1,000; and
(b) in addition to (a) and (a-a), conduct EDD under AML 7.1.1 in respect of:
(i) each customer it has assigned as high risk;
(ii) business relationships and transactions with persons from countries with high geographical risk factors.

(…)

11-1. DIGITAL ASSET TRANSFER (the "Travel Rule")
11-1.1. Digital Asset transfer definition
(1) A Digital Asset transfer is a transaction carried out:
(a) by a Digital Asset Trading Facility Operator or Digital Asset Service Provider (an "ordering institution") on behalf of an originator by transferring any Digital Assets; and
(b) with a view to making the Digital Assets available
(i) to that Person or another Person (a "beneficiary"); and
(ii) at an institution (a "beneficiary institution") which may be the ordering institution or another institution, whether or not one or more other institutions ("intermediary institutions") participate in completion of the transfer of the Digital Assets.

11-1.2. Obligations of Ordering Institution
(1) Before carrying out both a cross-border or domestic Digital Asset transfer of the amount equal to or above USD 1,000, an ordering institution must obtain, record and ensure that the transfers are accompanied by the following information:
(a) the name of the originator;
(b) the number of the originator's account maintained with the ordering institution and from which the Digital Assets are transferred or, in the absence of such an account, a unique reference number assigned to the Digital Asset transfer by the ordering institution;
(c) the originator's address, or national identity number, or customer identification number, or date and place of birth;
(d) the name of the beneficiary (recipient); and
(e) the number of the recipient's account maintained with the beneficiary institution and to which the Digital Assets are transferred or, in the absence of an account number, a unique transaction number assigned to the Digital Asset transfer by the beneficiary institution.
(2) Before carrying out both a cross-border or domestic Digital Asset transfer of the amount below USD 1,000, an ordering institution must obtain, record and ensure that the transfers are accompanied by the following information:
(a) the name of the originator;
(b) the number of the originator's account maintained with the ordering institution and from which the Digital Assets are transferred or, in the absence of such an account, a unique reference number assigned to the Digital Asset transfer by the ordering institution;
(c) the name of the beneficiary (recipient); and
(d) the number of the recipient's account maintained with the beneficiary institution and to which the Digital Assets are transferred, or, in the absence of an account number, a unique transaction number assigned to the Digital Asset transfer by the beneficiary institution.

(3) Before transferring Digital Assets, an ordering institution must verify the accuracy of the information referred to in (1) (a) to (c) on the basis of documents, data or information obtained from a reliable and independent sources.
(4) If several individual domestic or cross-border Digital Asset transfers from a single originating institution are bundled in a batch file for te transmission to recipient(s), then a Digital Asset Trading Facility Operator or Digital Asset Service Provider that is an ordering institution must ensure that:
(i) the batch file contains the originator information required in (1) and/or (2) respectively;
(ii) it has verified the originator information referred to in (1); and
(iii) the batch file contains the recipient information required under (1) and/or (2) for each recipient and that information is fully traceable in each recipient's jurisdiction.
(5) The information referred to in (1), (2), (4) must be submitted in advance of, or simultaneously or concurrently with, the transfer of Digital Assets and in a secure manner and in line with the requirements of the AIFC rules and regulations on data protection.

Guidance:
(1) The number of the account maintained with the ordering institution or beneficiary institution from or to which the Digital Assets are transferred referred to in 11-1.2.(1)(b) to (e) and 11-1.2.(2)(b) to (d) could mean:
(a) the originator's or recipients' Digital wallet (address), where a transfer of Digital Assets is registered on a network using distributed ledger technology or similar technology or,
(b) the originator's or beneficiary's account number, where such an account exists and is used to process the Digital Asset transaction if a transfer of Digital Asset is not registered on a network using distributed ledger technology or similar technology;
(b) Where information both in (1) (a) and (b) exists, ordering or beneficiary institutions should obtain, hold and/or send all information.

11-1.3. Obligations of Beneficiary Institution
(1) A Digital Asset Trading Facility Operator or Digital Asset Service Provider, which acts as a beneficiary institution in a Digital Asset transfer must obtain, record and implement effective procedures, including, where appropriate, monitoring during or after the transfer, in order to detect whether the referred to in 11-1.1(1) and (2) respectively, on the originator and the beneficiary is included in, or follows, the transfer of Digital Assets or batch file transfer.
(2) Before making the Digital Assets available to the beneficiary, for a Digital Asset transfer of amount equal to or above USD 1,000, a beneficiary institution must verify the accuracy of information of the recipient referred to in 11-1.1.(1)(d), on the basis of documents, data or information obtained from a reliable and independent sources.

11-1.4. Transfers of Digital Assets with missing or incomplete information on the originator or the beneficiary
(1) A Digital Asset Trading Facility Operator or Digital Asset Service Provider of the beneficiary must implement effective risk-based procedures, including procedures based on the risk-sensitive basis, for determining whether to execute or reject or suspend a transfer of Digital Asset that is not accompanied with a required complete originator and beneficiary information and for taking the appropriate follow-up action.
(2) Where the Digital Asset Trading Facility Operator or Digital Asset Service Provider of the beneficiary becomes aware that the information referred to in 11-1.1(1) and (2) is missing or incomplete, the Digital Asset Trading Facility Operator or Digital Asset Service Provider must before making the Digital Assets available to the beneficiary, on a risk-sensitive basis and without undue delay:
(a) reject the transfer or return the transferred Digital Assets to the originator's account; or
(b) ask for the required information on the originator and the beneficiary before making the Digital Assets available to the beneficiary.
(2) Where a Digital Asset Trading Facility Operator or Digital Asset Service Provider repeatedly fails to provide the required information on the originator or the beneficiary, the Digital Asset Trading Facility Operator or Digital Asset Service Provider of the beneficiary must:

(a) take steps, which may initially include the issuing of warnings and setting of deadlines; or
(b) reject any future transfers of Digital Assets from or to, or restrict or terminate its business relationship with, a provider of Digital Assets transfers that fails to provide the required information. The Digital Asset

Trading Facility Operator or Digital Asset Service Provider of the beneficiary must report that failure, and the steps taken, to the competent authority responsible for monitoring compliance with these Rules.

11-1.5. Digital Asset Transfers to or from self-hosted digital wallets

(1) In the case of a transfer of Digital Assets made to or received from on behalf of its a self-hosted digital wallet(s), the Digital Asset Service Provider of the originator or beneficiary must obtain and hold information referred to in in (1) or (2) from clients and ensure that the transfer of Digital Assets can be individually identified.

(2) In case of a Digital Asset transfer whose amount exceeds USD 1,000 or there is a suspicion of money laundering of a transfer to a self-hosted digital wallet Digital Asset Service Provider of the originator or beneficiary must take adequate measures on a risk-sensitive basis to mitigate and manage the ML/TF risks associated with the transfers.

Guidance on risk mitigating measures on transfers to or from self-hosted digital wallets

Digital Asset Service Provider should undertake following measures (non-exhaustive) to ensure compliance with (2):

(a) conduct enhanced monitoring of Digital Asset transfers with self-hosted digital wallets;

(b) accept Digital Asset transfers only from or to self-hosted digital wallets that the Digital Asset Service Provider has assessed to be reliable, having regard to the screening results of the Digital Asset transactions and the associated digital wallets and the assessment results on the ownership or control of the self-hosted digital wallet by the originator or beneficiary; and

(c) impose transaction limits or prohibition.

11-1.6. Rules in Chapter 11-1. comes into operation 12 months after the adoption of the AIFC Rules on Regulation of Digital Asset Activities.

11-2. DIGITAL ASSET TRANSFER COUNTERPARTY DUE DILIGENCE AND ADDITIONAL MEASURES.

11-2.1. General requirements Digital Asset transfer counterparty due diligence

(1) When an Authorised Person conducts a Digital Asset transfer referred to in Chapter 11-1, the Authorised Person will be exposed to money laundering and terrorist financing risks associated with the institution which may be the ordering institution, intermediary institution or beneficiary institution involved in the Digital asset transfer ("Digital Asset transfer counterparty").

(2) To avoid sending or receiving Digital Assets to or from illicit actors or designated parties that had not been subject to appropriate CDD and screening measures of a Digital Asset transfer counterparty and to ensure compliance with the Travel Rule, an Authorised Person must conduct due diligence on the Digital Asset transfer counterparty to identify and assess the money laundering and terrorist financing risks associated with the Digital Asset transfers to or from the Digital Asset transfer counterparty and apply appropriate risk-based anti-money laundering and countering financing terrorism measures.

(3) An Authorised Person should conduct due diligence measures on a Digital Asset transfer counterparty before conducting a Digital Asset transfer, or making the transferred Digital Assets available to the recipient.

(4) An Authorised Person does not need to undertake the Digital Asset transfer counterparty due diligence process for every individual Digital Asset transfer when dealing with Digital Asset transfer counterparties that it has already conducted counterparty due diligence on previously, unless when there is a suspicion of money laundering and terrorist financing.

(5) An Authorised Person undertakes reviews of the Digital Asset transfer counterparty due diligence records on a regular basis or upon trigger events (e.g., when it becomes aware of a suspicious transaction or other information such as negative news from credible media, public information that the counterparty has been subject to any targeted financial sanction, money laundering and terrorist financing investigation or regulatory action).

(6) Based on the Digital Asset transfer counterparty due diligence results, the Authorised Person determines if it should continue to conduct Digital Asset transfers with, and submit the required information to, a Digital Asset transfer counterparty, and the extent of anti-money laundering and countering financing terrorism measures that it should apply in relation to Digital Asset transfers with the Digital Asset transfer counterparty on a risk-sensitive basis.

11-2.2. Digital Asset transfer counterparty due diligence procedures

Digital Asset transfer counterparty due diligence typically involves the following procedures:

(a) determining whether the Digital Asset transfer is or will be with a Digital Asset transfer counterparty or a Self-Hosted Digital wallet;

(b) where applicable, identifying the Digital Asset transfer counterparty (e.g., by making a reference to lists of licensed or registered Digital Asset Service Providers or financial institutions in different jurisdictions); and

(c) assessing whether the Digital Asset transfer counterparty is an eligible counterparty to deal with and to send the required information to.

11-2.3. Digital Asset transfer counterparty due diligence measures

An Authorised Person applies the following Digital Asset transfer counterparty due diligence measures before it conducts a Digital Asset transfer with a Digital Asset transfer counterparty:

(a) determines if the respondent entity is licensed or registered;

(b) collects sufficient information about the Digital Asset transfer counterparty to enable it to understand fully the nature of the Digital Asset transfer counterparty's business;

(c) understands the nature and expected volume and value of Digital Asset transfers with the Digital Asset transfer counterparty;

(d) determines from publicly available information the reputation of the Digital Asset transfer counterparty and the quality and effectiveness of the anti-money laundering and countering financing terrorism regulation and supervision over the Digital Asset transfer counterparty by authorities in the jurisdictions in which it operates and/or is incorporated which perform functions similar to those of the competent authorities;

(e) assesses the anti-money laundering and countering financing terrorism controls of the Digital Asset transfer counterparty and ensures that the anti-money laundering and countering financing terrorism controls of the Digital Asset transfer counterparty are adequate and effective;

(f) assesses whether the Digital Asset transfer counterparty is subject to the Travel Rule similar to that imposed under Chapter 11-1 in the jurisdictions in which the Digital Asset transfer counterparty operates and/or is incorporated;

(g) assesses the adequacy and effectiveness of the anti-money laundering and countering financing terrorism controls that the Digital Asset transfer counterparty has put in place for ensuring compliance with the Travel Rule;

(h) assesses whether the Digital Asset transfer counterparty can protect the confidentiality and integrity of personal data (e.g., the required originator and recipient information), taking into account the adequacy and robustness of data privacy and security controls of the Digital Asset transfer counterparty; and

(j) obtains approval from its senior management.

Guidance:

(1) While a relationship with a Digital Asset transfer counterparty is different from a cross-border correspondent relationship referred to in Chapter 10, there are similarities in the due diligence approach which can be of assistance to an Authorised Person. By virtue of this, the Authorised Person should conduct the due diligence measures in Chapter 10, with reference to the requirements set out in AML 10.2.

(2) When assessing money laundering and financing terrorism risks posed by a Digital Asset transfer counterparty, an Authorised Person should take into account relevant factors that may indicate a higher money laundering and financing terrorism risk. Examples of such risk is where a Digital Asset transfer counterparty:

(i) operates or is incorporated in a jurisdiction posing a higher risk or with a weak anti-money laundering and countering financing terrorism regime;

(ii) is not (or yet to be) licensed or registered and supervised for anti-money laundering and countering financing terrorism purposes in the jurisdictions in which it operates and/or is incorporated by authorities which perform functions similar to those of the competent authorities;

(iii) does not have in place adequate and effective anti-money laundering and countering financing terrorism systems, including measures for ensuring compliance with the Travel Rule;

(iv) does not implement adequate measures or safeguards for protecting the confidentiality and integrity of personal data; or

(v) is associated with money laundering and financing terrorism or other illicit activities.