AMENDMENTS № 7.1

AIFC AUTHORISED MARKET INSTITUTION RULES

Approval Date: 9 December 2023

Commencement Date: 1 January 2024

In this document, underlining indicates a new text and strikethrough indicates a removed text.

(…)

Guidance: Purpose and application of AMI

(…)

The application of the rules in AMI is as follows:

- Chapter 1 contains introductory provisions applicable to all Authorised Market Institutions.
- Chapter 2 contains rules and guidance applicable to all Authorised Market Institutions.
- Chapter 2-1 contains rules and guidance applicable to Authorised Market Institutions Operating a facility for Security Tokens.
- Chapter 3 contains additional rules and guidance applicable to Authorised Investment Exchanges.
- Chapter 4 contains additional rules and guidance applicable to Authorised Clearing Houses (including Authorised Central Counterparties).
- Chapter 5 contains rules in relation to the supervision of Authorised Market Institutions.
- ~~Chapter 6 contains additional rules and guidance applicable to Authorised Digital Assets Trading Facility.~~
- Chapter 7 contains additional rules and guidance applicable to Authorised Crowdfunding Platforms.

(…)

(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.

(2) An Authorised Investment Exchange is a Centre Participant which has been licensed by the AFSA to carry on the Market Activity of Operating an Investment Exchange.

(3) An Authorised Clearing House is a Centre Participant which has been licensed by the AFSA to carry on the Market Activity of Operating a Clearing House.

(4) A central counterparty is a legal Person that interposes itself between the counterparties to the contracts traded on one or more financial markets, becoming the buyer to every seller and the seller to every buyer.

(5) An Authorised Central Counterparty is a central counterparty which is declared by an order made by the AFSA under these Rules for the time being in force to be an Authorised Central Counterparty.

(6) A Member of an Authorised Market Institution is a Person who is entitled, under an arrangement or agreement between him and the Authorised Market Institution, to use that institution's facilities.

(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.~~

(8) An Authorised Crowdfunding Platform is a Centre Participant which has been licensed by the AFSA to carry on the Market Activity of Operating a Loan Crowdfunding Platform and/or Operating an Investment Crowdfunding Platform.

(9) Operating a facility for Security Tokens in relation to an Authorised Market Institution means Operating an Investment Exchange on which Security Tokens are traded or Operating a Clearing House on which Security Tokens are cleared.

(…)

2.5.1. Requirement to prepare Business Rules

(…)

(2) An Authorised Market Institution must incorporate into its Business Rules the substance of any additional provisions to be found in the COB Rules, with any modifications which are appropriate, for the purpose of regulating the conduct of business of a Person referred to in AMI 2.6.1(1)(c) as a Member of the Institution for the purposes of dealing in Commodity Derivatives or Environmental Instruments.

(3) An Authorised Market Institution must incorporate into its Business Rules the substance of additional provisions to be found in the COB Rules, for the purpose of regulating the conduct of business of a Person referred to in AMI 2.6.1(1)(d) as a Member of the Institution for the purposes of dealing in Security Tokens.

(…)

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 categorised as 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;

(c) a Person intending to deal in Commodity Derivatives or Environmental Instruments who meets the criteria in GEN 1.1.14; or

(d) a Person not referred to in (a), (b), and (c) with access to the facility, on which Security Tokens are traded or cleared or both traded and cleared, in respect of their trading or clearing of Security Tokens only.

(2) An Authorised Market Institution must ensure that a Member who is a Person referred to in (1)(c) is a Professional Client and treat the Person as such.

For the purposes of this rule, Professional Client has the same meaning as defined in COB Chapter 2.

(3) Before admitting a Person referred to in (1)(c) as a Member, an Authorised Market Institution must undertake due diligence to ensure that such a Person:

(a) is of sufficient good repute;

(b) has a sufficient level of competence, experience and understanding of relevant Investments, Financial Services, transactions and any associated risks, including appropriate standards of conduct for its staff permitted to use its order entry system; and

(c) has adequate organisational arrangements, including financial and technological resources, which are appropriate to allow it to discharge its obligations in respect of their category of membership at the Authorised Market Institution.

(4) An Authorised Market Institution must keep records of the procedures which it has followed under (3), including any documents that evidence the Person's assessment. The records must be kept for at least six years from the date on which the business relationship with a Person ended.

(5) Before admitting a Person referred to in (1)(d), an Authorised Market Institution must undertake due diligence to ensure that the Person:

(a) is of sufficient good repute;

(b) has a sufficient level of competence, experience and understanding of relevant Investments, Financial Services, transactions and any associated risks, including appropriate standards of conduct for its staff permitted to use its order entry system;

(c) has adequate financial and technological resources to meet the Business Rules of the facility;

(d) does not pose any operational risks to the orderly and efficient functioning of the facility's trading or clearing systems; and

(e) does not pose any money laundering or terrorist financing risks.

(…)

2-1. RULES APPLICABLE TO AUTHORISED MARKET INSTITUTIONS OPERATING A FACILITY FOR SECURITY TOKENS

Guidance

Operating a facility for Security Tokens is defined in GLO as Operating an Exchange or Operating a Clearing House on which Security Tokens are traded, cleared, or both traded and cleared.

2-1.1. Technology and governance requirements

2-1.1.1. Without limiting the generality of the technology resources requirements in AMI 2.4, an Authorised Market Institution must:

(a) establish and maintain policies and procedures to ensure that any DLT application used in connection with the facility operates on the basis of 'permissioned' access, such that it allows the operator to have and maintain adequate control over the Persons who are permitted to access and update records held on that DLT application;

(b) establish and maintain adequate measures to ensure that the DLT application it uses, and the associated rules and protocols, contain:

(i) clear criteria governing Persons who are permitted to access and update records for the purposes of trading or clearing Security Tokens on the facility, including criteria about the integrity, credentials and competencies appropriate to the roles played by such persons;

(ii) measures to address risks, including to network security and network compatibility, that may arise through systems used by Persons permitted to update the records on the DLT application;

(iii) processes to ensure that the Authorised Market Institutions undertakes sufficient due diligence and adequate monitoring of ongoing compliance, relating to the matters referred to in (i) and (ii); and

(iv) measures to ensure there are appropriate restrictions on the transferability of Security Tokens in order to address AML and CFT risks;

(c) ensure any DLT application used for its facility is fit for purpose; and

(d) have regard to industry best practices in developing its technology design and technology governance relating to DLT that is used by the facility.

Guidance

1. To be fit for purpose, the technology design of the DLT application used by an Authorised Market Institution Operating a facility for Security Tokens should be able to address how the rights and obligations relating to the Security Tokens traded on that facility are properly managed and capable of being exercised or performed. For example, where a Security Token confers rights and obligations substantially similar to those conferred by a Share in a company, the DLT application would generally need to enable the management and exercise of the shareholder's rights. These

may, for example, include the right to receive notice of, and vote in, shareholder meetings, receive any declared dividends and participate in the assets of the company in a winding up.

2. To ensure the technology governance of any DLT application used on its facility is fit for purpose, an Authorised Market Institution should, as a minimum, have regard to the following:

a. careful maintenance and development of the relevant systems and architecture in terms of its code version control, implementation of updates, issue resolution, and regular internal and third party testing;

b. security measures and procedures for the safe storage and transmission of data in accordance with agreed protocols;

c. procedures to address changes in the protocol which result in modifications of or the splitting of the underlying distributed ledger into two or more separate ledgers (often referred to as a 'forks'), whether or not the new protocol is backwards compatible with the previous version;

d. procedures to deal with system outages, whether planned or not, and errors;

e. decision-making protocols and accountability for decisions;

f. procedures for establishing and managing interfaces with Digital wallet Service Providers; and

g. whether the protocols, smart contracts and other inbuilt features of the DLT application meet at least a minimum acceptable level of reliability and safety requirements, including to deal with a cyber or hacking attack, and how any resulting disruptions would be resolved.

3. Credentials which indicate a Person is suitable to update records for the purposes of trading or clearing Security Tokens on the facility may include:

a. accreditation by a recognised and reputable body to certify the requisite knowledge required; or

b. accreditation by the relevant body to certify compliance with the Kazakhstani standards in the area.

2-1.2. Operating a facility for Security Tokens that permits direct access

2-1.2.1. An Authorised Market Institution must ensure that:

(1) it treats each Direct Access Member as its Client;

(2) its Business Rules clearly set out:

(a) the duties owed by the Authorised Market Institution to the Direct Access Member and how the Authorised Market Institution is held accountable for any failure to fulfil those duties; and

(b) the duties owed by the Direct Access Member to the Authorised Market Institution and how the Direct Access Member is held accountable for any failure to fulfil those duties,

(3) appropriate investor redress mechanisms are available, and disclosed, to each Member permitted to trade or clear Security Tokens on its facility; and

(4) its facility contains a prominent disclosure of the risks associated with the use of DLT for trading and clearing Investments, particularly those relating to Digital wallets and the susceptibility of private cryptographic keys to misappropriation.

2-1.2.2. (1) Without limiting the generality of the systems and controls obligations of the Authorised Market Institution, an Authorised Market Institution must have in place adequate systems and controls to address market integrity, AML, CFT and investor protection risks in permitting a Direct Access Member to access its facility, including procedures to:

(a) identify the ultimate beneficial owner of a Direct Access Member, where the Member is a Body Corporate;

(b) ensure that appropriate due diligence sufficient to address AML and CFT risks has been conducted on each Direct Access Member, before permitting that Member to access its facility;

(c) detect and address market manipulation and abuse; and

(d) ensure that there is adequate disclosure relating to the Security Tokens that are traded on the facility, through prospectus and ongoing disclosure under chapters 1 and 6 of MAR.

(2) An Authorised Market Institution must have adequate controls and procedures to ensure that trading in Security Tokens by Direct Access Members does not pose any risks to the orderly and efficient functioning of the facility's trading system, including controls and procedures to:

(a) mitigate counterparty risks that may arise from defaults by Direct Access Members, through adequate collateral management measures, such as margin requirements, based on the settlement cycle adopted by the Authorised Market Institution;

(b) identify and distinguish orders that are placed by Direct Access Members, and, if necessary, enable the Authorised Market Institution to stop orders of, or trading by, such Direct Access Members;

(c) prevent Direct Access Members from allowing any other Persons to access the facility through that Direct Access Member's access; and

(d) ensure that Direct Access Members fully comply with the Business Rules of the facility and promptly address any gaps and deficiencies that are identified.

(3) An Authorised Market Institution must have adequate resources and mechanisms to carry out front-line monitoring of the trading activities of Direct Access Members and must be able to deal with any threats to market integrity appropriately.

(4) An Authorised Market Institution must ensure that, to the extent that any of the systems and controls referred to in (1) are embedded within, or otherwise facilitated through, DLT, they must be included within the scope of the annual audit and written report required under AMI 2-1.5.

2-1.2.3. When an Authorised Market Institution Executes a Transaction in Security Tokens for a Direct Access Member, the Authorised Market Institution must comply with the requirements relating to confirmation notes that would apply to an Authorised Firm under COB 9.1.2, 9.1.3 and 9.1.5.

2-1.3. Safe custody of Security Tokens

2-1.3.1. Without limiting the generality of AMI 2.9, where an Authorised Market Institution's obligations include making provision for the safeguarding and administration of Security Tokens belonging to Members and other participants on its facility, it must ensure that:

(1) where its safe custody arrangements involve acting as a Digital wallet Service Provider, it complies with the Client Asset provisions in COB 8.2 and 8.3 and the following requirements for firms Providing Custody of Security Tokens:

(a) A Digital wallet Service Provider must ensure that:
  (i) any DLT applications it uses in Providing Custody of Security Tokens are resilient, reliable and compatible with any relevant facility on which those Security Tokens are traded or cleared;
  (ii) it has the ability to clearly identify and segregate Security Tokens belonging to different Clients; and
  (iii) 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.
(b) A Digital wallet Service Provider, in developing and using DLT applications and other technology to Provide Custody of Security Tokens, must ensure that:
  (i) the architecture of any Digital wallets used adequately addresses compatibility issues and associated risks;
  (ii) 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 Security Tokens;
  (iii) 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;
  (iv) 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
  (v) the technology is compatible with the procedures and protocols built into the Operating Rules or equivalent on any facility on which the Security Tokens are traded or cleared or both traded and cleared.

(2) where it appoints a third party Digital wallet Service Provider to Provide Custody for Security Tokens traded or cleared on its facility, that Person is either:

(a) an Authorised Firm permitted to be a Digital wallet Service Provider; or

(b) a firm that is regulated by a Financial Services Regulator to an equivalent level as that provided for under the AFSA regime for Digital wallet Service Providers.

2-1.4. Technology audit reports

2-1.4.1. An Authorised Market Institution must:

(a) appoint a suitably qualified and independent third party professional to:

(i) carry out an annual audit of the Authorised Market Institution'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 (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 (a)(ii) within 4 months of the Authorised Market Institution's financial year end; and

(c) be able to satisfy the AFSA that the independent third party professional who undertakes the annual audit has the relevant expertise to do so, including by reference to the due diligence undertaken by the Authorised Market Institution to satisfy itself of that fact.

Guidance

Where an Authorised Market Institution appoints a third party professional for the purposes of (a)(i) and (ii), the Authorised Market Institution is expected to ensure that the professional is suitably qualified.

Credentials which indicate a qualified and independent third party professional is suitable to conduct audits of technology governance 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); or

(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.