Appendix 5

In this appendix underlining indicates new text and striking through indicates deleted text.

The DFSA Rulebook

Conduct of Business Module

(COB)

….

3   CORE RULES – INVESTMENT BUSINESS, ACCEPTING DEPOSITS, PROVIDING CREDIT, PROVIDING TRUST SERVICES, OPERATING A CROWDFUNDING PLATFORM, OPERATING AN EMPLOYEE MONEY PURCHASE SCHEME, ACTING AS THE ADMINISTRATOR OF AN EMPLOYEE MONEY PURCHASE SCHEME, PROVIDING MONEY SERVICES AND ARRANGING OR ADVISING ON MONEY SERVICES

….

3.3   Key information and Client Agreement

Application

3.3.1   The Rules in this section do not apply to an Authorised Firm when it is:

(a)   carrying on a Financial Service with or for a Market Counterparty;

(b)   Accepting Deposits;

(c)   Providing Credit;

(d)   carrying on an activity of the kind described in GEN Rule 2.26.1 that constitutes marketing;

(e)   a Fund Manager of a Fund Offering the Units of a Fund it manages;

(f)   Operating an Employee Money Purchase Scheme; or

(g)   Acting as the Administrator of an Employee Money Purchase Scheme; or

(h)   an ATS Operator.

….

6 ADDITIONAL RULES - INVESTMENT BUSINESS

….

6.11 CLIENT ASSETS

….

General requirements

6.11.2 (1) An Authorised Firm which holds or controls Client Money must comply with sections 6.12 and 6.14.

(2) An Authorised Firm which holds or controls Client Investments or Provides Custody must comply with sections 6.13 and 6.14.

(3) An Authorised Firm which Arranges Custody must comply with the requirements in Rule A6.5.1A (on suitability of non-DIFC custodians) and A6.7.1(1) (on disclosure) in APP 6 and in section 6.14 (Record keeping).

Guidance

Where an Authorised Firm holds or controls Client Investments which are Security Tokens, or Provides Custody in respect of Security Tokens, it must comply with the requirements in section 14.3 (in addition to those in 6.13 and 6.14).

….

6.12 Client money

….

Client money provisions

6.12.2 (1) An Authorised Firm in Category 4 must not hold Client Money, except if it does so in connection with it Operating an Alternative Trading System, Operating a Crowdfunding Platform or providing Money Transmission.

(2) An Authorised Firm which holds or controls Client Money for a Client must, subject to (3), comply with the Client Money Provisions in App5.

(3)   Where the Client is a Market Counterparty, an Authorised Firm may exclude the application of the Client Money Provisions but only where it has obtained the prior written consent of the Market Counterparty to do so.

Guidance

1. Providing Money Transmission is an activity that is included in the Financial Service of Providing Money Services – see the definition in GEN Rule 2.6.1(2).

2. In accordance with GEN chapter 8, an Authorised Firm which holds or controls Client Money must arrange for a Client Money Auditor's Report and, if it is Providing Money Services, a Money Services Auditor's Report to be submitted to the DFSA on an annual basis.

….

9   ADDITIONAL RULES: OPERATING AN ALTERNATIVE TRADING SYSTEM

9.1   Application and interpretation

9.1.1   This chapter applies to an Authorised Firm which Operates an Alternative Trading System (ATS Operator).

Guidance

1. The Financial Service of Operating an Alternative Trading System can be either operating a Multilateral Trading Facility (MTF) or operating an Organised Trading Facility (OTF). See GEN Rule 2.22.1.

2. This chapter will also apply to an ATS Operator that is Operating a Facility for Security Tokens, unless otherwise specified. Such an ATS Operator will also be subject to the additional requirements in chapter 14, as applicable.

9.1.2   In this chapter:

(a)   a reference to a "member" is a reference to a Client of the ATS Operator who has been granted access to its facilities in accordance with the requirements in this chapter and, unless otherwise specified, includes a Direct Access Member;

(b)   a reference to a "facility" is a reference to a Multilateral Trading Facility (MTF) and an Organised Trading Facility (OTF), except where specific reference is made only to an MTF or OTF;

(c)   a reference to an "ATS Operator" is a reference to a Person operating an MTF and a Person operating an OTF, except where specific reference is made only to a Person operating an MTF or a Person operating an OTF; and

(d)   where a Rule in this chapter conflicts with any other provision in the DFSA Rulebook, the Rule in this chapter prevails over those other provisions.

Guidance

Under Rule 9.3.1(1)(e), an ATS Operator that is Operating a Facility for Security Tokens is permitted to admit certain additional Persons as a member, where their access is only for trading or clearing of Security Tokens. Such Persons are defined in GLO and referred to in this module as Direct Access Members.

….

9.3   Member access criteria

9.3.1   (1)   An ATS Operator may, subject to (2), and (3) and (4), only accept as a member:

(a)   an Authorised Firm;

(b)   a Recognised Member;

(c)   a Person who meets the criteria in GEN Rule 2.3.2(2); or

(d)   a Person who is classified as a Professional Client pursuant to COB Rule 2.3.4(1)(g), (h) and (i); or

(e)   a Person not referred to in (a) to (d), only if:

(i)   the facility is one on which Security Tokens are traded; and

(ii)   the Person's access is only for trading Security Tokens.

(2)   An ATS Operator must not admit a Person referred to in (1)(c) or (d) unless such Person:

(a)   agrees in writing to submit unconditionally to the jurisdiction of the DFSA in relation to any matters which arise out of or which relate to its use of the facility;

(b)   agrees in writing to submit unconditionally to the jurisdiction of the DIFC Courts in relation to any proceedings in the DIFC, which arise out of or relate to its use of the facility;

(c)   agrees in writing to subject itself to the DIFC laws and the jurisdiction of the DIFC Courts in relation to its use of the facility; and

(d)   appoints and maintains at all times an agent for service of process in the DIFC and requires such agent to accept its appointment for service of process.

(3)   Prior to admitting a Person referred to in (1)(c) or (d) as a member, an ATS Operator must undertake due diligence to ensure that such a Person:

(a)   is of sufficiently good repute;

(b)   has a sufficient level of competence and experience; and

(c)   has adequate organisational arrangements, including financial and technological resources, which are no less than those required of an Authorised Firm appropriate to the nature of its operations.

(4)   Prior to admitting a Person referred to in 1(e), an ATS Operator must undertake due diligence to ensure that the Person:

(a)   meets the criteria in (3)(a) and (b);

(b)   has adequate financial and technological resources to meet the Operating Rules of the facility; and

(c)   does not pose any operational risks to the orderly and efficient functioning of the facility's trading systems.

Guidance

1.   See also the requirements relating to Direct Access Members in section 14.2.

2.   Members who are not Direct Access Members may also trade in Security Tokens.

Direct electronic access

9.3.2   An ATS Operator must have adequate rules and procedures to ensure that:

(a)   a Direct Access Member does not allow any other Person to have Direct Electronic Access to the facility; and

(b)   in any other case, its members do not allow any other Person to have Direct Electronic Access to the facility unless such other Person meets the requirements in Rule 9.3.1(1).

9.3.3   An ATS Operator must, where it permits any of its members to provide to another Person Direct Electronic Access to its facilities, have adequate systems and controls including:

(a)   appropriate standards regarding risk controls and thresholds on trading through Direct Electronic Access;

(b)   mechanisms to identify and distinguish orders placed by those Persons who are allowed to place orders through Direct Electronic Access; and

(c)   if necessary, the ability to stop orders of, or trading by, the Persons allowed Direct Electronic Access.

....

9.4   Investment criteria

9.4.1   An ATS Operator must ensure in respect of every Investment traded on its facility that:

(a)   only Investments which meet the requirements in (i), ~~or~~ (ii) or (iii) are ~~permitted to be~~ traded on its facility:

   (i)   in the case of Securities, the ~~only~~ Securities ~~which~~ are admitted to trading on an Authorised Market Institution or other Regulated Exchange; ~~or~~

   (ii)   in the case of Securities that are Security Tokens that do not meet the criteria in (i):

      (A)   there is a current Approved Prospectus relating to the Security Tokens;

      (B)   both the Security Tokens and the Reporting Entity of those Security Tokens meet the general eligibility requirements of MKT section 9.3;

      (C)   the ATS Operator has imposed requirements on the Reporting Entity of the Security Tokens, equivalent to those imposed on a Listed Entity under MKT sections 9.2 (the Listing Principles), 9.7 (continuing obligations, including disclosure) and 9.8 (provision of information to the DFSA); and

      (D)   the ATS Operator has adequate systems and controls in place to effectively monitor and enforce a Reporting Entity's compliance with the requirements imposed in (C); or

   (iii)   in the case of Derivatives, ~~only~~ the Derivatives are instruments that meet the contract specification criteria set out in AMI Rule 6.3.2;

(b)   there is sufficient information relating to the Investments traded on the facility available to members and other Persons having access to the facility through such members to enable such Persons to make informed decisions relating to such Investments; and

(c)   if it is an Investment that references to an underlying benchmark or index provided by a Price Information Provider, the requirements in Rule 9.4.2 are met.

….

9.6   Proper Markets

….

Prevention of Market Abuse

9.6.9 (1) An ATS Operator must:

(a) implement and maintain appropriate measures to identify, deter and prevent Market Abuse on and through its facility; and

(b) report promptly to the DFSA any Market Abuse.

(2) For the purposes of (1)(a), an ATS Operator must:

(a) include in its Operating Rules a regime to prevent Market Abuse, which is applicable to its members and their Clients; and

(b) implement and maintain adequate measures to ensure that its members comply with that regime.

(3) The regime to prevent Market Abuse referred to in (2)(a) must, at a minimum, include rules and procedures in relation to compliance with the applicable requirements in Part 6 of the Market Law, including adequate compliance arrangements applicable to its members and staff and the clients of members, record keeping, transaction monitoring, risk assessment and appropriate training.

Guidance

1. An ATS Operator should have an effective surveillance system in place for:

   a. the coordinated surveillance of all activity on or through its facilities and activity in related Investments conducted elsewhere; and

   b. communicating information about Market Abuse or suspected abuse, to the DFSA or appropriate regulatory authorities.

2. In determining whether an ATS Operator is ensuring that business conducted on its facilities is conducted in an orderly manner, the DFSA will consider:

   a. arrangements for pre and post trade transparency taking into account the nature and liquidity of the Investments traded; and

   b. the need to provide anonymity for trading participants.

3. An ATS Operator will also have appropriate procedures allowing it to influence trading conditions, suspend trading promptly when required, and to support or encourage liquidity when necessary to maintain an orderly market. The DFSA will consider the transparency of such procedures and the fairness of their application and potential application.

4. An ATS Operator that is Operating a Facility for Security Tokens must, where relevant, ensure measures under Rule 9.6.9(1) include effective measures to identify, deter and prevent Market Abuse by Persons permitted to access and update records held on any DLT or similar technology based application used in connection with the operation of its facility.

....

9.8   Use of 'security token market' and similar terms to refer to a facility

9.8.1 An ATS Operator must not refer to a facility it operates as a 'security token market', 'investment token market', 'derivative token market', or using any other similar term, unless it is a facility on which only Security Tokens are traded.

Guidance

For example, an ATS Operator must not refer to a facility where both Security Tokens and conventional Investments are traded using terms referred to Rule 9.8.1.

….

14 ADDITIONAL REQUIREMENTS FOR FIRMS PROVIDING FINANCIAL SERVICES RELATING TO SECURITY TOKENS

14.1 Technology and governance requirements for Operating a Facility for Security Tokens

14.1.1 Without limiting the generality of the technology resources requirements in section 9.5, an Authorised Firm Operating a Facility for Security Tokens must:

(a) 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; and

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

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

(4) 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 Firm 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 Firm 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 the splitting of the underlying distributed ledger into two or more separate ledgers (often referred to as a 'fork'), whether or not the new protocol is backwards compatible with the previous version (soft fork) or not (hard fork), and access to information where such a fork is created;

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

   e. decision-making protocols and accountability for decisions;

   f. procedures for the establishing and managing interfaces with providers of Digital Wallets; 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.

14.2 Operating a Facility for Security Tokens which permits direct access

Application

14.2.1 This section applies to an ATS Operator (referred to in this section as an "operator") that has Direct Access Members.

Guidance

1. A Direct Access Member is defined in GLO to mean a Person that ATS an admitted as a member under COB Rule 9.3.1(1)(e).

2. See also the requirements relating to Direct Access Members in Rule 9.3.1(4).

Requirements

14.2.2 An operator must ensure that:

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

(2)   its Operating Rules clearly set out:

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

(b)   the duties owed by the Direct Access Member to the operator and how the member is held accountable for any failure to fulfil those duties; and

(3)   appropriate investor redress mechanisms are available, in accordance with GEN chapter 9, and disclosed to each member permitted to trade Security Tokens on its facility.

14.2.3 (1)   Without limiting the generality of the systems and controls obligations of the operator, an operator must have in place adequate systems and controls to address market integrity, AML, CTF or investor protection risks in permitting a Direct Access Member to trade on its facility, including procedures to:

(a)   identify the ultimate beneficial owner of a Direct Access Member, where such a member is a body corporate;

(b)   ensure that appropriate customer due diligence sufficient to address AML and CTF risks has been conducted on each Direct Access Member, prior to permitting that member to trade on its facility;

(c)   detect and address market manipulation and abuse;

(d)   ensure that there is adequate disclosure relating to the Security Tokens that are traded on the facility, including through prospectus and on-going disclosure under MKT chapters 2, 4 and 6.

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

(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 operator;

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

(c)   prevent Direct Access Members allowing access to other persons to trade on the trading facility; and

(d)   ensure that Direct Access Members fully comply with the Operating Rules of the facility and that where gaps and deficiencies are identified, they are promptly addressed, in accordance with Rule 9.3.4.

(3)   An operator must have adequate resources and mechanisms to carry out front-line monitoring of trading activities by Direct Access Members.

(4)   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 associated report required under Rule 14.5.1.

Guidance

1.   To satisfy the DFSA of the matters referred to in Rule 14.2.3(1), an operator should, at a minimum, be able to demonstrate that it has built into its DLT or similar technology application being used, or otherwise implemented, effective procedures that enable:

   (a)   the clear identification of each Direct Access Member accessing its facility to trade; and

   (b)   the monitoring of bid and offer prices and volatility for any indications of market manipulation or abuse.

14.3 Requirements for firms Providing Custody of Security Tokens

Interpretation

14.3.1 In this section:

   (a)   Digital Wallet Service Provider means an Authorised Firm Providing Custody in respect of Security Tokens by holding and controlling the public and private cryptographic keys relating to the Security Tokens;

   (b)   Third Party Digital Wallet Service Provider means:

      (i)   a Digital Wallet Service Provider other than an ATS Operator Providing Custody in respect of Security Tokens traded on its facility; or

      (ii)   a Person in another jurisdiction Providing Custody in respect of Security Tokens by holding and controlling the public and private cryptographic keys relating to the Security Tokens, that is authorised and supervised for that activity by a Financial Services Regulator; and

   (c)   Self Custody of Security Tokens means the holding and controlling of Security Tokens by their owner, through that owner holding and controlling the public and private cryptographic keys relating to those Security Tokens.

Application

14.3.2 This section applies to an Authorised Firm which is a Digital Wallet Service Provider.

Guidance

1. A Security Token is an Investment, as defined in GEN Rule A2.1.1. The Financial Service of Providing Custody, as defined in GEN Rule 2.13.1, therefore includes Providing Custody of a Security Token, and a Person carrying on that Financial Service will require a Licence to do so.

2. An Authorised Firm which is Providing Custody of Security Tokens is, in addition to the requirements in this section, subject to other relevant requirements that apply to a firm Providing Custody of Investments. Other applicable requirements include the Client Assets requirements in section 6.11, the Client Investments requirements in section 6.13 and the Safe Custody Provisions in App 6.

3. The Rules in this section will not apply to a Person providing a Digital Wallet to a Person who uses it for Self Custody of Security Tokens, as the Security Tokens in that Digital Wallet are then held and controlled by that Person at their own risk.

Requirements

14.3.3 (1) A Digital Wallet Service Provider must ensure that:

(a) 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;

(b) it has the ability to clearly identify and segregate Security Tokens 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, in developing and using DLT applications and other technology to Provide Custody of Security Tokens, must ensure that:

(a) the architecture of any Digital Wallets 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 Security Tokens;

(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 Operating Rules or equivalent on any facility on which the Security Tokens are traded or cleared or both traded and cleared.

Guidance

Where an Authorised Firm that is a Digital Wallet Service Provider delegates any function to a Third Party Digital Wallet Service Provider, it must ensure that the delegate fully complies with the requirements of Rule 14.3.3. The outsourcing and delegation requirements of GEN Rule 5.3.21 and 5.3.22 would also apply to the Authorised Firm in those circumstances.

14.3.4   An ATS Operator that appoints a Third Party Digital Wallet Service Provider to Provide Custody of Security Tokens traded on its facility, must ensure that the 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 of regulation as provided for under the DFSA regime for Providing Digital Wallet Services.

Guidance

Where an ATS Operator appoints a non-DIFC firm regulated by a Financial Services Regulator, it must undertake sufficient due diligence to establish that the non-DIFC firm is subject to an equivalent level of regulation as under the DFSA regime in respect of that service.

14.3.5   A Digital Wallet Service Provider must ensure that the annual report required under Rule 14.5.1 includes confirmation as to whether it has complied with the requirements set out in Rule 14.3.3.

14.4   Provision of key features document relating to Security Tokens

Application

14.4.1   This section applies to an Authorised Firm which carries on any one or more of the following Financial Services in respect of Security Tokens:

(a)   Dealing in Investments as Principal;

(b)   Dealing in Investments as Agent;

(c)   Arranging Deals in Investments;

(d)   Managing a Collective Investment Fund;

(e)   Managing Assets;

(f)   Advising on Financial Products;

(g)   Providing Custody; or

(h)   Arranging Custody.

14.4.2 (1)   An Authorised Firm must not provide a Financial Service to which this section applies to a Person unless it has provided that Person with a key features document containing the information in (2).

(2)   The key features document must contain the following information in respect of each Security Token relevant to the Financial Services that the Authorised Firm will provide to the Person:

(a)   the risks associated with and essential characteristics of the Issuer (or other Person responsible for discharging the obligations associated with the rights conferred), and guarantor if any, of the Security Token, including their assets, liabilities and financial position;

(b)   the risks associated with and essential characteristics of the Security Token, including the rights and obligations conferred and the type or types of Investment which it constitutes;

(c)   whether the Security Token is or will be admitted to trading and if so, the details relating to such admission, including details of the facility and whether the facility is within the DIFC;

(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, particularly 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 Security Token, and any related risks (for example, at whose risk the Client's Security Tokens 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 Security Tokens such as voting or participation in shareholder actions; and

(h)   any other information relevant to the particular Security Token that 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 Financial Service is provided to the Person, to enable that Person to make an informed decision about whether to use the relevant Financial 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.

14.5   Technology audit reports

14.5.1 (1)   This Rule applies to an Authorised Firm where it:

(a)   is Operating a Facility for Security Tokens;

(b)   holds or controls Client Investments and those Investments include Security Tokens; or

(c)   is reliant on DLT or similar technology to carry on one or more of the Financial Services specified at Rule 14.4.1 in respect of Security Tokens.

(2)   An Authorised Firm specified in (1) 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, including those specified in this Chapter; 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 DFSA a copy of the report referred to in (a)(ii) within 4 months of the Authorised Firm's financial year end; and

(c)   be able to satisfy the DFSA 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 Firm to satisfy itself of that fact.

Guidance

An Authorised Firm may appoint an Auditor to carry out the functions specified in (a)(i) and (ii), provided it has satisfied itself that Auditor has the relevant expertise required to do so.

….