FINANCIAL SERVICES REGULATORY AUTHORITY

Guidance – Regulation of Crypto Asset Activities in ADGM

DATE: 14 May 2019
Table of Contents
INTRODUCTION.................................................................................................................................. 4
BACKGROUND...................................................................................................................................... 5
OBJECTIVES OF THE OCAB FRAMEWORK...................................................................................... 7
FEATURES OF THE OCAB FRAMEWORK .......................................................................................... 8
Regulated Activity of Operating a Crypto Asset Business................................................................. 8
OCAB Holders as Authorised Persons ............................................................................................. 9
Combination of Regulated Activities .............................................................................................. 10
REGULATORY REQUIREMENTS FOR OPERATING A CRYPTO ASSET BUSINESS......................... 11
Operating a Crypto Asset Business ................................................................................................. 11
Accepted Crypto Assets .................................................................................................................... 11
Capital Requirements ...................................................................................................................... 13
Anti-Money Laundering and Countering Financing of Terrorism .................................................... 14
International Tax Reporting Obligations .......................................................................................... 22
Technology Governance and Controls ......................................................................................... 22
Maintenance and development of systems..................................................................................... 23
Security measures and procedures ................................................................................................. 23
Origin and destination of Crypto Asset funds .................................................................................. 25
Planned and Unplanned system outages ......................................................................................... 26
Management of personnel and decision making .......................................................................... 27
Third party outsourcing .................................................................................................................. 27
Forks ................................................................................................................................................. 28
Crypto Asset Risk Disclosures ......................................................................................................... 28
Market Abuse, Transaction Reporting and Misleading Impressions (FSMR) ................................... 30
SPECIFIC FSRA GUIDANCE ON THE OCAB FRAMEWORK .......................................................... 30
Application of particular Rules in COBS ......................................................................................... 30
Substance requirements of OCAB Holders ....................................................................................... 31
Crypto Asset Brokers or Dealers ....................................................................................................... 31
Appointment of adviser .................................................................................................................... 32
Certain class order modifications / waivers .................................................................................... 32
Data protection obligations for OCAB Holders .............................................................................. 33
Transactions with unknown counterparties ...................................................................................... 34
Margin trading ................................................................................................................................. 34
Insurance ........................................................................................................................................ 35
CRYPTO ASSET EXCHANGES ......................................................................................................... 35
Recognised Investment Exchanges Operating a Crypto Asset Exchange ........................................ 42
CRYPTO ASSET CUSTODIANS ......................................................................................................... 42

FSRA OCAB Guidance Version 2.0
INTRODUCTION

1) This Guidance is issued under section 15(2) of the Financial Services and Markets Regulations 2015 ("FSMR"). It should be read in conjunction with FSMR, the relevant Rulebooks of the Financial Services Regulatory Authority ("FSRA"), the FSRA’s Guidance & Policies Manual and its ‘Guidance – Regulation of Initial Coin/Token Offerings (ICOs) and Crypto Assets under the FSMR’ ("ICO Guidance").

2) This Guidance is applicable to the following Persons:

   a) an Applicant for a Financial Services Permission ("FSP") to carry on the Regulated Activity of Operating a Crypto Asset Business ("OCAB") in or from the Abu Dhabi Global Market ("ADGM");

   b) an Authorised Person in respect of its carrying on the Regulated Activity of Operating a Crypto Asset Business in or from ADGM;

   c) a Recognised Investment Exchange with a stipulation on its Recognition Order permitting it to carry on the Regulated Activity of Operating a Crypto Asset Business within ADGM; or

   d) an Applicant/Authorised Person in respect of the use of stablecoins in or from ADGM.

3) This Guidance sets out the FSRA’s approach to the regulation of Crypto Asset activities in ADGM, including activities conducted by Crypto Asset Exchanges, Crypto Asset Custodians and Crypto Asset intermediaries. This Guidance, together with the applicable ADGM Regulations and FSRA Rules governing Crypto Asset activities, is collectively referred to as the “OCAB Framework”.

4) This Guidance is not an exhaustive source of the FSRA’s policy on the exercise of its regulatory functions and powers. The FSRA is not bound by the requirements set out in this Guidance and may –

   a) impose additional requirements to address any specific risks posed by Crypto Asset activities;

   b) waive or modify any of the Rules relevant to the OCAB Framework, at its discretion, where appropriate.

5) Unless otherwise defined or the context otherwise requires, the terms contained in this Guidance have the same meaning as defined in the FSMR and the FSRA Glossary Rulebook ("GLO").

1 http://adgm.complinet.com/net_file_store/new_rulebooks/g/u/Guidance_ICOs_and_Crypto_Assets_13052019.pdf
2 Refer to the section on stablecoins, starting at paragraph 158.
6) For the purposes of this Guidance, an Authorised Person holding an FSP to carry on the Regulated Activity of Operating a Crypto Asset Business, or a Recognised Investment Exchange holding an OCAB stipulation on its Recognition Order (as set out in paragraph 131) is referred to as an “OCAB Holder”.

7) For more details on the process for authorisation as an OCAB Holder operating a Crypto Asset Exchange, please contact the FSRA at MIP@adgm.com. For more details on the process for authorisation as an OCAB Holder for any other Crypto Asset business activities, please contact the FSRA at authorisation@adgm.com.

BACKGROUND

8) Technological innovation is transforming the financial services industry. Constant advances in new technologies have provided opportunities for significant change and disruption to financial services and other related activities globally. Developments in distributed ledger technologies (“DLT”) have led to the emergence of various types of digital assets, including virtual coins or tokens for capital raising, and crypto assets for the facilitation of economic transactions or the transfer of value.

9) This Guidance primarily focuses on the FSRA’s regulatory treatment of Crypto Assets, and the types of Crypto Asset related financial services activities that can be conducted within ADGM. For the purposes of the OCAB Framework, the FSRA has defined Crypto Assets in the FSMR as follows:

“Crypto Asset” means a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. A Crypto Asset is -

(a) neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Crypto Asset; and

(b) distinguished from Fiat Currency3 and E-money4."

10) The diagram and table on the following pages set out the FSRA’s regulatory approach in relation to different types of digital assets.

[3] “Fiat Currency” means government issued currency that is designated as legal tender in its country of issuance through government decree, regulation or law.

The FSRA regulates, and will allow to operate within the ADGM, the Digital Assets located within the blue dotted line and Derivatives over/Funds investing in Digital Assets.

<table>
<thead>
<tr>
<th>Category of Digital Assets / Instruments</th>
<th>Regulatory Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Digital Securities” (e.g., digital/virtual tokens that have the features and characteristics of a Security under the FSMR (such as Shares, Debentures and Units in a Collective Investment Fund))</td>
<td>Deemed to be Securities pursuant to Paragraph 58(2)(b) of FSMR. All financial services activities in relation to Digital Securities, such as operating primary / secondary markets, dealing / trading / managing investments in or advising on Digital Securities, are subject to the relevant regulatory requirements under the FSMR. Market intermediaries and market operators dealing or managing investments in Digital Securities need to be licensed / approved by FSRA as FSP holders (including as MTFs), Recognised Investment Exchanges or Recognised Clearing Houses, as applicable.</td>
</tr>
<tr>
<td>“Crypto Assets” (e.g., non-fiat virtual currencies, crypto ‘exchange tokens’). As stated in paragraph 9, this Guidance is primarily focused on Crypto Assets.</td>
<td>Treated as commodities and, therefore, not deemed Specified Investments under the FSMR. Pursuant to the OCAB Framework, however, market intermediaries (e.g., broker dealers, custodians, asset managers) dealing in or managing Crypto Assets, and Crypto Asset Exchanges, need to be licensed / approved by FSRA as OCAB Holders. Only activities in Accepted Crypto Assets will be permitted. Capital formation activities are not provided for under the OCAB Framework, and such activities are not envisaged under the Market Rules (MKT).</td>
</tr>
</tbody>
</table>
Market intermediaries and market operators dealing in such Derivatives and Collective Investment Funds will need to be licensed / approved by FSRA as FSP holders, Recognised Investment Exchanges or Recognised Clearing Houses, as applicable.

“Utility Tokens”
(e.g., tokens which can be redeemed for access to a specific product or service, typically provided using a DLT platform, do not exhibit the features and characteristics of a regulated investment / instrument under the FSMR).

Treated as commodities and, therefore, not deemed Specified Investments under the FSMR.

Unless such Utility Tokens are caught as Accepted Crypto Assets, spot trading and transactions in Utility Tokens do not constitute Regulated Activities, activities envisaged under a Recognition Order (e.g., those of a Recognised Investment Exchange or Recognised Clearing House), or activities envisaged under MKT.

“Fiat Tokens”
(e.g. stablecoins whose value are fully backed by underlying fiat currencies)

Treated as a form of digital representation of Fiat Currency.

Where used as a payment instrument for the purposes of Money Transmission as defined under the FSMR, the activity will be licensed and regulated as Providing Money Services.

11) For clarification, the OCAB Framework is not intended to apply to initial token or coin offerings (ICOs), (whether Digital Securities or Utility tokens), or other capital formation/capital raising purposes. For details on FSRA’s regulatory treatment of ICOs, digital Securities and utility tokens please refer to the FSRA’s ICO Guidance.

OBJECTIVES OF THE OCAB FRAMEWORK

12) Fiat currencies are created and issued by sovereign governments, and stored and transferred by banks and other regulated financial institutions on behalf of users. In contrast, the crypto asset ecosystem can enable users to create, store and transfer Crypto Assets without the need for any third party. This creates a set of unique challenges for regulators worldwide. Without regulated entities controlling the creation and use of Crypto Assets, the system is open to significant Financial Crime and other risks.

13) The OCAB Framework is comprehensive in order to effectively address the key risks that the trading of Crypto Assets poses. FSRA’s view is that regulation of AML/CFT risks alone will not sufficiently mitigate certain wider Crypto Asset related risks. Given the increased use of Crypto Assets as a medium for financial transactions, and their connectivity to the mainstream financial system through Crypto Asset and Derivative exchanges and intermediaries, there is the increased potential of contagion risks impacting the stability of the financial sector. There is also no current safety net that ensures that users will be able to recover their Crypto Assets in case of loss or theft.
14) Accordingly, the FSRA has addressed issues around consumer protection, safe custody, technology governance, disclosure/transparency, Market Abuse and the regulation of Crypto Asset Exchanges in a manner similar to the regulatory approach taken in relation to securities/derivatives exchanges globally.

FEATURES OF THE OCAB FRAMEWORK

Regulated Activity of Operating a Crypto Asset Business

15) In accordance with section 30 of FSMR, Applicants that qualify for authorisation under the OCAB Framework will be granted an FSP to carry on the Regulated Activity of OCAB. The Regulated Activity of OCAB, and the relevant exclusions, are set out in sections 73B, 73C and 73D of Schedule 1 of FSMR, and in full below:

‘Operating a Crypto Asset Business

(1) Operating a Crypto Asset Business is a specified kind of activity.

(2) Operating a Crypto Asset Business involves undertaking one or more Crypto Asset activities in or from the Abu Dhabi Global Market.

(3) For the purposes of sub-paragraph (2), Crypto Asset activities include –
   (a) Buying, Selling or exercising any right in Accepted Crypto Assets (whether as principal or agent);
   (b) managing Accepted Crypto 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 Crypto Assets;
   (d) marketing of Accepted Crypto Assets;
   (e) advising on the merits of Buying or Selling of Accepted Crypto Assets or any rights conferred by such Buying or Selling; and
   (f) operating -
      (i) a Crypto Asset Exchange; or
      (ii) as a Crypto Asset Custodian.

(4) In sub-paragraph 3(f)(i), operating a Crypto Asset Exchange means the trading, conversion or exchange of -
   (a) Fiat Currency or other value into Accepted Crypto Assets;
   (b) Accepted Crypto Assets into Fiat Currency or other value; or
   (c) one Accepted Crypto Asset into another Accepted Crypto Asset.

(5) In sub-paragraph 3(f)(ii), operating as a Crypto Asset Custodian involves -
(a) safeguarding, storing, holding or maintaining custody of Accepted Crypto Assets belonging to another person; or
(b) controlling or administering Accepted Crypto Assets for the purpose of sub-paragraph 5(a).

Exclusions
The following activities do not constitute Operating a Crypto Asset Business—
(1) the creation or administration of Crypto Assets that are not Accepted Crypto Assets;
(2) the development, dissemination or use of software for the purpose of creating or mining a Crypto Asset;
(3) the transmission of Crypto Assets;
(4) a loyalty points scheme denominated in Crypto Assets; or
(5) any other activity or arrangement that is deemed by the Regulator to not constitute Operating a Crypto Asset Business, where necessary and appropriate in order for the Regulator to pursue its objectives.

Order Routing
A person does not operate a Crypto Asset Exchange if its operates a facility which is merely an order routing system where Buying and Selling interests in, or orders for, Accepted Crypto Assets are merely transmitted but do not interact.’

OCAB Holders as Authorised Persons
16) To be authorised as an OCAB Holder, an Applicant must satisfy FSRA that all applicable requirements of FSMR and the relevant FSRA Rulebooks have been, and will continue to be, complied with. Upon authorisation, an OCAB Holder, as a holder of an FSP, is an Authorised Person for the purposes of the FSMR and the FSRA Rulebook, and has the same regulatory status within ADGM as any other Authorised Person.

17) The principal Rules for Operating a Crypto Asset Business are set out in Chapter 17 of the FSRA Conduct of Business Rulebook (“COBS”). Though the requirements set out in COBS Rule 17.1.2 already apply to Authorised Persons generally, COBS Rule 17.1.2 operates as a ‘sign-post’ Rule designed to draw the attention of Applicants and OCAB Holders to the fact that they must comply with all Rules applicable to Authorised Persons, including:

a) all other relevant chapters of COBS;
b) the FSRA General Rulebook (“GEN”);
c) the FSRA Anti-Money Laundering and Sanctions Rules and Guidance (“AML”); and
d) the FSRA Rules of Market Conduct (“RMC”).
18) The table below sets out the main risk areas, and the related mitigations for each of these risks areas, under the OCAB Framework.

<table>
<thead>
<tr>
<th>RISK</th>
<th>MITIGANT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. AML/CFT/TAX</td>
<td>The AML Rulebook applies in full to the Regulated Activity of OCAB. OCAB Holders also need to consider their reporting obligations in relation to FATCA and the Common Reporting Standards.</td>
</tr>
<tr>
<td>2. CONSUMER PROTECTION</td>
<td>All material risks associated with Crypto Assets generally, Accepted Crypto Assets and an OCAB Holders’ products, services and activities must be appropriately disclosed, and monitored and updated on an ongoing basis.</td>
</tr>
</tbody>
</table>
| 3. TECHNOLOGY GOVERNANCE | Systems and controls must be in place in relation to:  
- Crypto Asset wallets;  
- Private keys;  
- Origin and destination of Crypto Asset funds;  
- Security; and  
- Risk management and systems recovery. |
| 4. ‘EXCHANGE-TYPE’ ACTIVITIES | Crypto Asset Exchanges are regulated in a similar manner to how the FSRA regulates ‘Multilateral Trading Facilities’ (MTFs), and are required to have in place, among other things, the following:  
- Market surveillance;  
- Fair and orderly trading;  
- Settlement processes;  
- Transaction recording;  
- A rulebook(s);  
- Transparency & public disclosure mechanisms; and  
- Exchange-like operational systems and controls. |
| 5. CUSTODY | OCAB Holders that hold or control either Accepted Crypto Assets and / or Client Money (e.g., fiat currencies) under custody on behalf of Clients are subject to the Safe Custody and / or Client Money Provisions respectively under FSMR and COBS. Frequent reconciliations and reporting of Accepted Crypto Assets and Client Money, as well as appropriate internal controls to safeguard them, are required. |

19) COBS Rule 17.1.3 operates such that an OCAB Holder is deemed to be operating an ‘Investment Business’, and that ‘Client Investments’ in GEN and ‘Financial Instruments’ in RMC are read to include Crypto Assets. This means that the various Rules using these terms throughout the FRSA Rulebooks are expanded to capture Crypto Assets and Crypto Asset activities, including in particular the Rules contained in Chapters 3 and 6 of COBS.

**Combination of Regulated Activities**

20) Applicants approved by the FSRA to Operate a Crypto Asset Business will be granted an FSP that includes the Regulated Activity of OCAB. Applicants seeking to carry on other Regulated Activities, in addition to OCAB, within ADGM will need to apply to FSRA to add

---

5 That is not solely operating as a Crypto Asset Exchange (say, for example, a Crypto Asset OTC broker).
such other Regulated Activities to their FSP and comply with the requirements of the FSRA, including in relation to fees applicable to such other Regulated Activities in accordance with the FSRA FEES Rulebook.6

21) For example, OCAB Holders wishing to operate as a broker, dealer or custodian in the conventional space will need to apply for and hold the relevant licenses applicable to those conventional Regulated Activities, in addition to its OCAB license. In certain circumstances,7 where an OCAB Holder is using the same, or substantially similar, technology, systems and controls used for the operation of its Crypto Asset Activities (and as already approved by the FSRA as part of its OCAB license application) as proposed to be used for its conventional Regulated Activities, the FSRA may, in its sole discretion, consider a reduction in the fees associated with the license application for the additional conventional Regulated Activities being applied for.

22) Existing FSP holders carrying on a Regulated Activity that incidentally involves the use of Crypto Assets, but who are not deemed as carrying on OCAB activities as defined under the FSMR, may not need to apply for the Regulated Activity of OCAB8. In such circumstances, however, the FSP holder may be subject to relevant Rules in Chapter 17 of COBS (e.g., in relation to Accepted Crypto Assets, technology governance, disclosure requirements) to ensure that appropriate activity is undertaken as part of their non-OCAB Regulated Activities.

REGULATORY REQUIREMENTS FOR OPERATING A CRYPTO ASSET BUSINESS

Operating a Crypto Asset Business

23) Chapter 17 of COBS applies to all OCAB Holders, requiring compliance with all requirements set out in COBS Rules 17.1 – 17.6. OCAB Holders that are Operating a Crypto Asset Exchange or Operating as a Crypto Asset Custodian are also required to comply with the additional requirements set out in COBS Rules 17.7 or 17.8 respectively.

Accepted Crypto Assets

24) COBS Rule 17.2.1 permits OCAB Holders to engage in Crypto Asset activities in relation to Accepted Crypto Assets only. The FSRA has a general power to determine each Accepted Crypto Asset that will be permitted in relation to OCAB activities within ADGM, in order to prevent potential higher-risk activities relating to illiquid or ‘immature’ Crypto Assets.

25) A Crypto Asset that meets the FSRA’s requirements, as demonstrated by an individual OCAB Holder, will constitute an Accepted Crypto Asset for that individual OCAB Holder

---

6 Subject to paragraph 131 which notes that OCAB Holders operating a Crypto Asset Exchange who also wish to be authorised as a Recognised Investment Exchange must relinquish their FSP in order to obtain a Recognition Order with a stipulation allowing the holder to Operate a Crypto Asset Business, by way of operation of a Crypto Asset Exchange.

7 These circumstances include OCAB Holders operating a Crypto Asset Exchange and applying for a Recognition Order for a Recognised Investment Exchange in order to operate a Digital Securities market.

8 Including certain activities in relation to stablecoins (see paragraphs starting at paragraph 158).
only. COBS Rule 17.2.2 states that for the purpose of determining whether, in its opinion, a Crypto Asset meets the requirements of being an Accepted Crypto Asset, the FSRA will consider those factors it considers relevant, which at the date of this Guidance include seven key factors as set out below: 9

a) **Maturity / market capitalisation**: the market capitalisation\(^{10}\) of the Crypto Asset, the sufficiency, depth and breadth of Client demand, the proportion of the Crypto Asset that is in free float, and the controls/processes to manage volatility of a particular Crypto Asset;

b) **Security**: consideration of whether a specific Crypto Asset is able to withstand, adapt, respond to, and improve on its specific risks and vulnerabilities, including relevant factors/risks relating to the on-boarding or use of new Crypto Assets (including size, testing, maturity, and ability to allow the appropriate safeguarding of secure private keys);\(^{11}\)

c) **Traceability / monitoring**: whether OCAB holders are able to demonstrate the origin and destination of the specific Crypto Asset, if the Crypto Asset enables the identification of counterparties to each transaction, and if on-chain transactions in the Crypto Asset can be adequately monitored;

d) **Exchange connectivity**: whether there are (other) exchanges that support the Crypto Asset; the jurisdictions of these exchanges and whether these exchanges are suitably regulated;

e) **Type of Distributed Ledger (DLT)**: whether there are issues relating to the security and/or usability of a DLT used for the purposes of a Crypto Asset; whether the Crypto Asset leverages an existing DLT for network and other synergies; whether a new DLT has been demonstrably stress tested;

f) **Innovation / efficiency**: whether, for example, the Crypto Asset helps to solve a fundamental problem, addresses an unmet market need or creates value for network participants; and

g) **Practical application/functionality**: whether the Crypto Asset possesses real world, quantifiable, functionality.

26) Though these factors may change from time to time, the FSRA will, in all cases, have regard to its objectives as a regulator, and the principles as set out in Section 1 of FSMR.

\(^{9}\) Factor (a) relates to COBS Rule 17.2.2(a), with factors (b)-(g) relating to COBS Rule 17.2.2(b).

\(^{10}\) The FSRA does not prescribe the source for calculating the market capitalisation of a Crypto Asset and will consider certain recognised sources, as may be available from time to time.

\(^{11}\) OCAB Holders will be required to undertake third party verification to demonstrate that the Crypto Assets it is proposing to use meet the security requirements applicable to being deemed an Accepted Crypto Asset. A similar verification requirement will also apply to any stablecoins/fiat tokens proposed to be used by an Applicant/OCAB Holder – see paragraph 162.
27) Applicants applying for an FSP will need to submit the details of each Accepted Crypto Asset that is proposed to be used for their OCAB activities, setting out separately for each proposed Crypto Asset how it meets the tests set out in paragraph 25 above. The use of each Accepted Crypto Asset will be approved as part of the formal application process for its FSP for Operating a Crypto Asset Business.

28) An Accepted Crypto Asset may be deemed suitable for use by more than one OCAB Holder, subject to each OCAB Holder satisfying the FSRA that it can meet the regulatory requirements in respect of the specific Accepted Crypto Asset. For example, a Crypto Asset Exchange is required by COBS Rule 17.7.412 to notify the FSRA of any new Accepted Crypto Asset proposed to be admitted to trading on its facilities. Though the Crypto Asset Exchange may propose to admit to trading a commonly used and traded Crypto Asset, the Crypto Asset Exchange’s controls, for example, relating to identity/transaction monitoring of a certain distributed ledger may not yet be fully developed. In such circumstances, the FSRA may require the Crypto Asset Exchange to delay the commencement of trading until such time that suitable controls have been developed and implemented.

29) An OCAB Holder wishing to use a Crypto Asset(s) additional to the Accepted Crypto Asset(s) originally approved as part of its application process, must first seek the FSRA’s approval before offering it to Clients. This application should be made in writing and include all relevant information relating to the use of the Crypto Asset, including the relevant controls the OCAB Holder has in place (or if not already in place, that it proposes to implement), in order to manage any risks specific to the Crypto Asset. In forming a view on the suitability of the proposed Crypto Asset(s), the FSRA will take into account whether the proposed Crypto Asset meets the requirements to be an Accepted Crypto Asset, as set out in COBS Rule 17.2.2 and paragraph 25 of this Guidance. The FSRA will notify the OCAB Holder of its determination.

30) Due to Accepted Crypto Assets being determined for use on the basis of each individual OCAB Holder, the FSRA will not maintain a ‘public’ list of Accepted Crypto Assets.

**Capital Requirements**

31) Given the nature of, and the risks associated with the Regulated Activity of Operating a Crypto Asset Business, COBS Rule 17.3 requires an OCAB Holder to hold regulatory capital in a manner consistent with MIR Rule 3.2.1 (being the requirements that a Recognised Investment Exchange must meet). Pursuant to these Rules, regulatory capital held by an OCAB Holder must be in fiat form.

32) When applying COBS Rule 17.3 / MIR Rule 3.2.1 to OCAB Holders, the FSRA will apply proportionality in considering whether any additional capital buffer must be held, based on the size, scope, complexity and nature of the Crypto Asset activities and operations of the OCAB Holder and, if so, the appropriate amount of regulatory capital required as an additional buffer. An OCAB Holder that the FSRA considers to be high risk may attract higher regulatory capital requirements.

---

12 Which requires notification to the FSRA under MIR Rule 5.4.1 (Item 26).
33) Subject to the above paragraph, in general:

a) OCAB Holders operating a Crypto Asset Exchange, are required to hold regulatory capital equivalent to 12 months’ operational expenses; and

b) all other OCAB Holders are required to hold regulatory capital equivalent to 6 months’ operational expenses.

34) Operational expenses, as set out in MIR Rule 3.2.1, broadly include all of the overhead, non-discretionary costs (variable and exceptional items can be excluded) incurred (or forecast to be incurred) by an OCAB Holder in its operations over the course of a twelve-month period. Technology-related operational expenses, such as the use of IT servers and technology platforms, storage and usage of IT equipment and technology services required for the overall operability of the OCAB Holders’ platform, are to be included. Development costs, such as research and intellectual property patenting can be excluded.

35) Where an OCAB Holder also carries on one or more conventional Regulated Activities (e.g., Dealing in Investments, Providing Credit or Providing Custody), the FSRA will apply a capital requirement that is the higher of the regulatory capital requirements applicable to:

a) OCAB; or

b) the other Regulated Activities under the FSRA Prudential – Investment, Insurance Intermediation and Banking Rules (“PRU”).

36) In addition, where an OCAB Holder is part of a wider financial Group that is subject to consolidated supervision by the FSRA, a holistic view of regulatory capital treatment will apply across the businesses of the Group pursuant to Chapter 8 of PRU. The resulting level of regulatory capital for the consolidated Group will also be subject to review under the Supervisory Review and Evaluation Process (as outlined in Chapter 10 of PRU), whereby the FSRA will retain the ability to impose additional capital requirements, above and beyond that reflected in the ‘higher of’ approach to reflect any part of the higher risk profile of the Group that is not adequately captured in Chapter 8 of PRU.

**Anti-Money Laundering and Countering Financing of Terrorism**

37) Crypto Asset activities raise significant regulatory concerns for regulatory authorities and law enforcement agencies worldwide, particularly in relation to Money Laundering (“ML”) and Terrorism Financing (“TF”). International bodies, such as the International Monetary Fund (“IMF”), the Financial Action Task Force (“FATF”), the Bank for International Settlements (“BIS”) and the International Organisation for Securities Commissions (“IOSCO”), have issued different Digital Asset (including Crypto Asset and ICO) warnings to investors and market participants advising of the significant risks, including ML and TF risks, and the possibility of Digital Assets being used for wider illegal purposes.
38) FATF has identified certain key risks associated with Crypto Assets\(^{13}\), which include the following:

a) Digital Assets (including, in particular, Crypto Assets) may operate in an anonymous or pseudo-anonymous manner. Crypto Assets can be traded via Internet platforms, are generally characterised by non-face-to-face Client relationships, and may permit (pseudo-)anonymous funding and transfers (cash funding or third-party funding through ‘virtual exchanges’ that may not properly identify the source or destination of funds);

b) The global reach of Crypto Assets increases the potential for ML/TF risks. Crypto Asset systems can be accessed via the Internet (including via mobile phones), and can be used to make cross-border payments and fund transfers;

c) Crypto Asset platforms commonly rely on complex infrastructures utilising several entities, often spanning multiple countries, to transfer funds or execute payments. This segmentation of services means that responsibility for ML/TF compliance and supervision/enforcement may be unclear. Moreover, Client and transaction records may be held by different entities, in different jurisdictions, making it more difficult for regulators and law enforcement agencies to access them. These issues are exacerbated by the rapidly evolving nature of ‘decentralised’ technologies used by Crypto Asset businesses, including the changing number and types/roles of participants providing services in the Crypto Asset ecosystem; and

d) Components of the Crypto Asset system may be located in jurisdictions that do not have adequate ML/TF controls.

39) On 22 February 2019, FATF issued a public statement recognising the need to adequately mitigate the ML and TF risks associated with digital asset activities\(^{14}\). As per the statement, FATF proposed more details relating to the regulation and supervision/monitoring of virtual asset services providers (“VASPs”)\(^{15}\) by way of its (Draft) Interpretive Note to Recommendation 15, “New technologies”.\(^{16}\)

40) The Key (Draft) Interpretive Notes to Recommendation 15 include:

a) Digital assets being considered as “property,” “proceeds,” “funds”, “funds or other assets,” or other “corresponding value”, requiring the application of relevant measures under the FATF Recommendations to digital assets and VASPs; and

---


\(^{14}\) Though the activities deemed by FATF as ‘virtual asset activities’ are wider, they do cover the activities deemed by FSRA as OCAB activities. FATF uses the term ‘virtual assets’, which for the purposes of (and consistency within) this Guidance has been replaced with the term ‘digital assets’.

\(^{15}\) For the purposes of this Guidance, VASPs, though a wider collection of entities, are treated similar to OCAB Holders.

\(^{16}\) The text of the new FATF Interpretive Note has been published for consultation, and, subject to amendment agreed under the consultation period, is expected to be formally adopted as part of the FATF Standards in June 2019.
b) VASPs being required to be licensed or registered in the jurisdiction(s) where they are created or in which they operate.

c) Recommendations 10 to 21 being proposed to directly apply to VASPs, subject to the following proposed qualifications/requirements:

i. **Recommendation 10** - The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1,000; and

ii. **Recommendation 16** - New requirements relating to the obligations of Originating VASPs and Beneficiary VASPs.17

41) In order to develop a robust and sustainable regulatory framework for Crypto Assets, FSRA is of the view that a comprehensive application of its Anti Money Laundering and Countering Financing of Terrorism “AML/CFT” framework should be in place, including full compliance with, among other things:

   a) UAE AML/CFT Federal Laws, including the UAE Cabinet Resolution No. (10) of 2019 Concerning the Executive Regulation of the Federal Law No. 20 of 2018 concerning Anti-Money Laundering and Combating Terrorism Financing;

   b) the FSRA AML and Sanctions Rules and Guidance (“AML Rules”) or such other AML rules as may be applicable in ADGM from time to time; and

   c) the adoption of international best practices (including FATF Recommendations).

42) Taking into account Crypto Asset ML and TF risks, the importance of meeting global transparency and beneficial ownership standards, and the need to have proper mechanisms to exchange information with other regulators and counterparties, the FSRA requires that its AML Rules apply to all OCAB Holders.

---

17 The FSRA Notes that the draft Recommendation 16 was published for consultation by FATF, and has been directly subject to public and private industry response. The FSRA continues to monitor the position of FATF in relation to Recommendation 16, and will consider how to adopt FATF’s finalised Recommendations upon their publication in due course. To summarise, Recommendation 16 proposes that:

- Originating VASPs should obtain and hold required and accurate originator information and required beneficiary information on digital asset transfers, submit the above information to beneficiary VASPs and counterparts (if any), and make it available on request to appropriate authorities. It is not necessary for this information to be attached directly to digital asset transfers;

- Beneficiary VASPs should obtain and hold required originator information, and required and accurate beneficiary information on digital asset transfers, and make it available on request to appropriate authorities; and

- Other requirements of Recommendation 16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis.
Key considerations for AML/CFT compliance

43) When considering the FATF Recommendations, in combination with the application of the AML Rules, the FSRA notes the following key principles that an OCAB Holder should consider:

Principle 1: Risk Based Approach

a) FATF expects countries, regulators, financial institutions and other concerned parties to adopt a ‘Risk Based Approach’ (“RBA”). OCAB Holders are expected to understand the risks associated with their activities and allocate proper resources to mitigate those risks. A RBA can only be achieved if it is embedded into the compliance culture of the OCAB Holder, which enables the OCAB Holder to make decisions and allocate appropriate resources in the most efficient and effective way.

b) OCAB Holders should, on a periodic basis, carry out a proper risk based assessment of their processes and activities. In order to implement the RBA, OCAB Holders are expected to have processes in place to identify, assess, monitor, manage and mitigate ML risks. The general principle is that in circumstances where there are higher risks of ML, OCAB Holders are required to implement enhanced measures to manage and mitigate those risks.

c) One of the most challenging risks facing financial institutions is how the on-boarding of an OCAB Holder may affect its relationship with foreign correspondent financial institutions, as well as the views of the regulator of those foreign correspondent financial institutions. In essence, a foreign correspondent financial institution relationship is built on the effectiveness of a financial institution’s ML compliance program and ongoing monitoring capabilities.

d) With the use of cryptology and block chain technologies at a nascent stage within financial services, any financial institution banking an OCAB Holder must not only satisfy itself, but also its foreign correspondent financial institution(s), that those OCAB Holders are well regulated and have appropriate systems and controls in place to address ML, TF and sanctions risks. These systems and controls should include robust processes to carry out CDD on Clients and beneficial owners, to monitor transactions for these risks, and the willingness and ability of the OCAB Holder to provide complete transparency to its financial institution(s) and foreign correspondent financial institution(s) if and when required.

Principle 2: Business Risk Assessment

e) Chapter 6 of the AML Rules requires Relevant Persons to take appropriate steps to identify and assess the ML risks to which their businesses are exposed, taking into consideration the nature, size and complexity of their activities. When identifying and assessing these risks, several factors should be considered, including an assessment of the use of new technologies. Importantly, in the context of Crypto Assets, FATF Recommendation (15) states that:
“Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.”

f) Another aspect of assessing the business risk relevant to OCAB Holders is gaining familiarity with the characteristics and terminology\(^\text{18}\) of the Crypto Asset industry. Additionally, OCAB Holders, and their management and staff, should be aware of the possible misuse of Crypto Assets in criminal activities, as well as the technical and complicated nature of Crypto Assets (and the platforms they operate on).

g) When making its assessment, an OCAB Holder must give consideration to all business risks. For example, while an issue may be identified in relation to cyber security (e.g., when dealing with hot wallets or using cloud computing to store data – being a ‘technology’ risk), the FSRA expects OCAB Holders to consider these risks from all perspectives to establish whether the risk triggers other issues for consideration (including ML/TF risks, technology governance and consumer protection). An OCAB Holder must then use the identified risks to develop and maintain its AML/CTF policies, procedures, systems and controls and take all reasonable steps to eliminate or manage such risks.

**Principle 3: Customer Risk Assessment and Customer Due Diligence**

h) The FSRA expects all OCAB Holders to have fully compliant Client on-boarding processes. Crypto Assets have been criticised by regulatory bodies globally due to their (pseudo-)anonymity features, which makes tracking Client records and transactions more challenging for compliance officers and money laundering reporting officers.

i) Customer Risk Assessment and ‘Customer Due Diligence’ (‘CDD’) policies and procedures are required to be implemented by all OCAB Holders. OCAB Holders should have a process to assess and rate all their Clients according to that Client’s risk profile (and taking into consideration the OCAB Holder’s RBA). This risk-based assessment is required to be undertaken for each Client prior to transacting any business on behalf of the Client. OCAB Holders must undertake CDD for each Client and comply in full with Chapter 8 of the AML Rules noting that the FSRA does not consider it appropriate for OCAB Holders to use simplified CDD when conducting Crypto Asset activities, largely due to issues surrounding the (pseudo-)anonymity of Clients and transactions associated with Crypto Assets.

\(^{18}\) Examples of Digital Asset/Crypto Asset relevant terminology include: cold, warm or hot wallets/storage, on/off ramps, tainted wallets, public key, private key and forks.
j) In case of non-face-to-face Client on-boarding and ongoing due diligence, the FSRA expects that OCAB Holders will take the necessary action, and develop appropriate policies, to ensure correct identification of a Client as a natural person. This may include obtaining a “selfie”, together with two currently valid forms of the Client’s facial ID; one must be the Client’s passport with all details clear and visible, the second should be a copy (front and back) of an official government issued document, such as a national ID or driver’s license.

k) The FSRA understands that OCAB Holders may need to use new technology to improve Client on-boarding processes for the purpose of assessing and managing ML and TF risks. For example, in order for OCAB Holders to conduct non-face-to-face on-boarding they will need to implement facial recognition software to validate the “selfie” against the other uploaded documentation, or other suitable biometric technology.

l) The FSRA further understands that the proper use of such technologies (e.g., fingerprinting, retinal/eye scans, use of real-time video conference facilities to enable facial recognition) can assist with mitigation of the ML/TF risks associated with Crypto Asset activities. Technological features, such as secure digital signatures that allow the verification of a Client’s identity through a signed document, may also be acceptable to the FSRA. In all cases, an OCAB Holder should ensure that the use of these technologies will not lead to a simplified process where the required Customer Risk Assessment and CDD requirements are not appropriately undertaken by an OCAB Holder.

m) The FSRA recommends that OCAB Holders obtain a signed self-certification from their Clients identifying the details of all passports issued and held in their name(s). OCAB Holders may also use this as an opportunity to capture all tax related details in order to meet their international tax reporting obligations. Self-certification should not prevent OCAB Holders from conducting proper CDD.

**Principle 4: Governance, Systems and Controls**

n) OCAB Holders are required to implement an appropriate governance structure, especially in relation to Information Technology governance, and provide for the development and maintenance of all necessary systems and controls to ensure appropriate ML and TF compliance.

o) The FSRA expects that OCAB Holders may seek to utilise (their own or third-party) technologies and solutions to meet their regulatory obligations (e.g., customer risk assessment, detection of fraud, and transaction identification, monitoring and reporting) and risk management requirements (e.g., margin limits, large exposure monitoring).

---

19 Please also refer to the section on Technology Governance and Controls in this Guidance (page 22).
p) The FSRA expects OCAB Holders to develop, implement and maintain effective transactional monitoring systems to determine the origin of a Crypto Asset and to monitor its destination, and to apply strong “know your transaction” measures which enable OCAB Holders to have complete granular data centric information about the transactions done by a Client.

q) The FSRA expects OCAB Holders to act responsibly and always be vigilant in ensuring that their activities are not subject to any misuse by participants transacting with Crypto Assets that may have been tainted in any way from an illegal activity. The FSRA expects that an OCAB Holder’s internal processes establish the types of ‘indicators’ or activities that could be used to identify when Accepted Crypto Assets may have been used in an illegal manner. An OCAB Holder should have a process for the management of when such ‘indicators’ (for example, certain Client or use of “mixer” and “tumbler” services) are triggered.

r) While the FSRA cannot recommend particular vendors or providers, all technology solutions must be fit for purpose and OCAB Holders should consider using those with an established track record, and undertake their own due diligence/risk assessment to ensure competency and capability. The FSRA recognises that many of the (technology) solutions appropriate for mitigating Crypto Asset risks are continuing to be developed within the Crypto Asset industry itself.

s) The FSRA expects OCAB Holders to develop, implement and adhere to a “Crypto Asset Compliance Policy”, tailored to meet specific Crypto Asset business compliance requirements, and reflecting a clear comprehension of the OCAB Holder’s understanding of its compliance responsibilities. The FSRA expects this policy to be well defined, comprehensive, robust and as specific to an individual OCAB Holder’s activities as possible. The policy can be separate or part of other compliance policies/manuals.

t) Following the development of the Crypto Asset Compliance Policy, OCAB Holders’ compliance officers are expected to establish a “Crypto Asset compliance monitoring program”, requiring internal reviews to be conducted in an efficient way, and on a periodic basis.

u) OCAB Holders must appoint a Money Laundering Reporting Officer (“MLRO”) who will be responsible for the implementation and oversight of the OCAB Holder’s compliance with the AML Rules. Consistent with the FSRA’s expectation in relation to all other Authorised Persons, an OCAB Holder’s MLRO should have an appropriate level of seniority and independence in order to be effective in the role.

**Principle 5: Suspicious Activity Reporting obligations**

v) OCAB Holders should familiarise themselves with their reporting obligations under the AML Rules, in particular in relation to the reporting of suspicious activities/transactions.
w) Prior to commencing operations, the FSRA expects OCAB Holders to establish online connectivity with the UAE’s Financial Intelligence Unit for the purposes of submitting Suspicious Activity Reports ("SARs"). Instructions on how to do this can be found on the FSRA’s FCPU webpage.

x) OCAB Holders are required to establish sophisticated transaction monitoring systems to detect possible ML and TF activities. Systems should also be implemented to effectively identify any attempt to breach domestic and international sanctions. Such systems may rely on new technological solutions (including monitoring algorithms or Artificial Intelligence (“AI”)).

Principle 6: Record keeping

y) As proper documentation is one of the main pillars of ensuring AML/CFT compliance, OCAB Holders are required to have policies and procedures in place to ensure proper record keeping practices. It is expected the OCAB Holder will maintain up to date records in accordance with the CDD obligations applicable to it and be prepared to provide the records upon request from the FSRA.

z) The FSRA understands that the transaction recording of many Crypto Asset transactions is linked to, or based on, DLT. This requires an OCAB Holder to implement specific arrangements to ensure that, at a minimum, the OCAB Holder and the FSRA have access to all relevant information as necessary. An OCAB Holder may use a distributed ledger to store its data, provided it is able to provide this data, in an easily accessible format, to the FSRA when required.

aa) The FSRA views Crypto Asset activities that are linked to cash transactions as posing higher ML and TF risks, due to the source of funding being significantly more difficult to determine. OCAB Holders wishing to conduct cash transactions will be required to implement enhanced controls to mitigate the inherent risks of such transactions. Such controls may include, among other things, setting appropriate limits on cash deposits (e.g., daily, monthly, yearly limits), a prohibition on receiving cash directly, prohibitions on the receipt of cash other than from bank accounts, and prohibitions on receiving funds from third parties. In all cases, OCAB Holders will need to clearly demonstrate to the FSRA how their controls suitably mitigate the risks of cash transactions within their operations. Considering the wider consumer protection implications, the FSRA also considers it unlikely to be appropriate for OCAB Holders to accept deposits by way of credit card or credit facilities/credit lines.

bb) FSRA expects all OCAB Holders to exercise due care, to the utmost extent possible, in their day-to-day operations and when dealing with Clients or potential Clients. An OCAB Holder’s activities are expected to be in compliance with the AML Rules, ensuring that their activities do not pose a regulatory risk or reputational damage to the ADGM Financial System.
International Tax Reporting Obligations

44) COBS Rule 17.4 requires OCAB Holders to consider and, if applicable, adhere to their tax reporting obligations including, as applicable, under the Foreign Account Tax Compliance Act (“FATCA”) and the ADGM Common Reporting Standard Regulations 2017.

Technology Governance and Controls

45) While the FSRA adopts a technology-neutral approach to its regulation of OCAB Holders, Crypto Asset technology is widely considered to be in its early years of development and usage at scale. While it does not seek to regulate Crypto Asset technology directly, the FSRA expects OCAB Holders to meet particular requirements in terms of their technology systems, governance and controls.

46) Historic Crypto Asset business failures have often arisen as a result of the lack of adequate technology-related procedures, including, for example, lack of security measures, systems development methodologies, limited system penetration testing for operating a robust business and lack of technical leadership and management. The FSRA has therefore included specific Guidance regarding expected controls and processes to help mitigate these issues.

47) GEN Rule 3.3 requires an OCAB Holder to establish systems and controls to ensure its affairs are managed effectively and responsibly, and to ensure such systems and controls are subject to continuous monitoring and review. COBS Rule 17.5 sets out additional requirements for appropriate technology governance and controls specific to OCAB Holders, with a focus on:

   a) Crypto Asset Wallets;
   b) Private Keys;
   c) Origin and destination of Crypto Asset funds;
   d) Security; and
   e) Risk Management.

48) When complying with GEN Rule 3.3 and COBS Rule 17.5, OCAB Holders should have due regard to the following key areas from a technology perspective:

   a) Careful maintenance and development of systems and architecture (e.g., 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;
c) Business continuity and Client engagement planning in the event of both planned and unplanned system outages;

d) Processes and procedures specifying management of personnel and decision-making by qualified staff; and

e) Procedures for the creation and management of services, interfaces and channels provided by or to third parties (as recipients and providers of data or services).

*Maintenance and development of systems*

49) OCAB Holders are expected to have a well-defined, documented and deliberate approach for the implementation and upgrade of systems and software.

50) OCAB Holders should also have well-established policies and procedures for the regular and thorough testing of any system currently implemented or being considered for use (e.g., upgrades to a matching engine or opening of a new Application Programming Interface (“API”) internally or with a third party).

51) The updated system should be tested for technical, operational and security vulnerabilities including but not limited to functional, penetration and stress testing. The outcome of the testing should be well structured and documented and signed off by the responsible (technology-focused) executives of the OCAB Holder.

52) All changes made to the codebase in use are to be tracked and recorded, with a clear audit trail for appropriate internal checks and sign-offs. The use of a version control system which allows for the accurate timestamping and identification of the user responsible for relevant changes should be considered.

53) OCAB Holders should maintain a clear and comprehensive audit trail for system issues internally, including security issues and those with third parties, their resolution and implementation of fixes.

54) OCAB Holders should conduct at least annual third-party verification/audit of core systems being used (including, if relevant, verification / audit of custody arrangements and verification of the amount of their purported holdings of Crypto Assets and Client Money). Crypto Asset Custodians and Crypto Asset Exchanges should have an annual review of their infrastructure undertaken by reputable third party cyber security consultants, producing a list of recommendations and areas of concern.

*Security measures and procedures*

55) OCAB Holders should have measures and procedures in place which comply with network security industry best practices (e.g., the implementation of firewalls, strong passwords, password management procedures, multifactor authentication and encryption of data in transit and at rest).
56) Updates and patches to all systems, particularly security systems, should be performed as soon as safely feasible after such updates and patches have been released, whether these systems have been developed internally or developed by a third-party.

57) Crypto Asset Exchange and Crypto Asset Custodian IT infrastructures are expected to provide strong layered security and seek the elimination of “single points of failure”. IT infrastructure security policies are required to be maintained, describing in particular how strong layered security is provided and how “single points of failure” are eliminated. This includes, but should not be limited to, systems and procedures to limit the access of a single user to the use of private and confidential information of Clients.

58) IT infrastructures should be strong enough to resist, without significant loss to Clients, a number of scenarios, including but not limited to: accidental destruction or breach of data, collusion or leakage of information by employees/former employees, successful hack of a cryptographic and hardware security module or server, or access by hackers of any single set of encryption/decryption keys that could result in a complete system breach.

59) OCAB Holders should have in place policies and procedures that address information security for all personnel. The security policy should set the security tone for the whole entity and inform personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. To mitigate “key person risk”, OCAB Holders are to ensure that there is no single individual that holds privileged or sensitive information that is critical to the operations of the OCAB Holder.

60) The strong encryption of data, both at rest and in transit, should be included in the security policy. In particular, encryption and decryption of Crypto Asset private keys should utilise strong encryption protocols and algorithms that have broad acceptance with cyber security professionals. Critical cryptographic functions such as encryption, decryption, generation of private keys, and the use of digital signatures should only be performed within cryptographic modules complying with the highest, and internationally recognised, applicable security standards.

61) All security incidents and breaches should be logged and documented in detail as soon as practicable and the resolution and implementation details should subsequently be added to the log.

62) The use of open source software should be governed by clear, well documented and transparent rules and procedures governing the software’s stability, security and fitness for purpose. Any open source software, whether it is a compiled distribution or code, should be thoroughly tested for security and operational vulnerabilities. This testing should be signed off by the responsible executives of the OCAB Holder before it is used for processing or storing of operational and Client information.

63) All APIs that are internal or external-facing should be secured by strict access management procedures and systems, including encryption of the information (e.g.,
SSL certificates). All API access activity should be logged and scanned for security breaches on an ongoing basis.

64) All access management and credential changes (for employees, third-party service providers and Clients) should be governed and monitored by strict and well documented rules and procedures. This should include, but not be limited to, enforcing strong passwords and the monitoring of IP geo-location, use of VPN, TOR or unencrypted web connections.

**Cryptographic Keys and wallet storage**

65) The ability to send and receive Crypto Assets by recording new transactions on a distributed ledger is usually dependent on cryptographic keys – a public key and one or more private keys. The public key allows other users on a distributed ledger to send Crypto Assets to an address associated with that public key. The private key(s) provides full control of the Crypto Assets associated with the public key. As such, OCAB Holders need to have robust procedures and protective measures to ensure the secure offline generation, storage, backup and destruction of both public and private keys for their own wallet operations and where they offer wallet services to Clients.

Whether private keys are held on network attached devices or devices that are offline, OCAB Holders must have policies and procedures to ensure that they are not compromised by malicious actors.

**Password protection and encryption**

66) OCAB Holders should consider the use of multi-signature wallets (e.g., where multiple private keys are associated with a given public key and a subset of these private keys, sometimes held by different parties, are required to authorise transactions). Where a multi-signature solution is not feasible due to the underlying structure of the Crypto Asset, a similar mechanism or procedure should be in place (e.g., a multi-user authentication prior to enacting on-chain changes to the Crypto Asset holdings).

67) OCAB Holders should have clear policies and procedures that detail procedures for recovery in the event that a Client loses access credentials. These policies and procedures should also cover the recovery or re-generation of lost private keys (e.g., using a seed phrase if applicable).

68) OCAB Holders must have policies and procedures in place that set out actions and responsibilities in the event of a breach of private and public keys, as well as Client user access credentials.

**Origin and destination of Crypto Asset funds**

69) Crypto Asset transactions between public addresses take place on public DLT. Although it is normally possible to identify the public addresses of the parties to a transaction, it is often very difficult to establish the owner (whether natural or legal)
of these addresses. This makes Crypto Assets attractive to money launderers, terrorist financiers and other criminals.

70) The US Office of Foreign Asset Control (OFAC) has issued a statement requiring wallet addresses known to belong to individuals listed on the Specially Designated Nationals And Blocked Persons sanctions (“SDN”) list to be reported. Further information is available on the OFAC website. Additionally, there are companies collecting “tainted” wallet addresses that have been used in hacks, “dark web” transactions and other criminal activities.

71) An OCAB Holder must have clear policies and procedures, consistent with the AML Rules applicable to it, to identify the source of funds and to ensure its compliance with COBS Rules 17.5(c) (Origins and destination of Crypto Asset funds) and 17.5(e) (Risk Management). These policies and procedures should cover due diligence on the deposits and withdrawals by legal persons that represent further multiple deposit-holders or withdrawal recipients of the Crypto Assets. For such deposits and withdrawals, OCAB Holders should be able to assess the ultimate beneficiaries’ wallet addresses and their source or destination of funds as appropriate.

72) It is crucial that OCAB Holders perform due diligence on their Clients before opening an account so that wallet addresses can be identified as belonging to a specific user. If a transaction is detected that originates from or is sent to a “tainted” wallet address belonging to a known user, that user should be reported. OCAB Holders should maintain lists of tainted wallet addresses and, if not in possession of their own services, utilise third party services to help identify such addresses.

73) Currently, there are technology solutions developed in-house and available from third party service providers which enable the tracking of Crypto Assets through multiple transactions to more accurately identify the source and destination of these Crypto Assets. It is expected that OCAB Holders may need to consider the use of such solutions and other systems to adequately meet their anti-money laundering, financial crime and know-your-customer obligations under the OCAB Framework.

Planned and Unplanned system outages

74) OCAB Holders should have a programme of planned systems outages to provide for adequate opportunities to perform updates and testing. OCAB Holders should also have multiple communication channels to ensure that its Clients are informed, ahead of time, of any outages which may affect them.

75) OCAB Holders should have clear, publicly available, procedures articulating the process in the event of an unplanned outage. During an unplanned outage, OCAB Holders should be able to rapidly disseminate key information and updates on a frequent basis.

21 For full details on these obligations, please refer to the earlier section of AML/CFT.
Management of personnel and decision making

76) OCAB Holders should implement processes and procedures concerning decision making and access to sensitive information and security systems.

77) A clear audit log of decision making should be kept. Staff with decision-making responsibilities should have the adequate expertise, particularly from a technological standpoint, to make such decisions.

78) Protective measures should be implemented to restrict access to critical and/or sensitive data to key personnel only. This includes both digital and physical access. OCAB Holders should have processes and procedures to track and monitor access to all network resources. Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimising the impact of a data compromise. The maintenance of logs allows thorough tracking, alerting, and analysis when issues occur.

Third party outsourcing

79) OCAB Holders may use third party services for their systems. However, when doing so, the OCAB Holder (pursuant to GEN 3.3.31) retains full responsibility from a regulatory perspective for any issues that may result from the outsourcing including the failure of any third party to meet its obligations. The FSRA requires that certain core systems (for example, the matching engine of a Crypto Asset Exchange) are maintained by the OCAB Holder itself and will not generally permit these to be outsourced.

80) In its assessment of a potential third party service provider, an OCAB Holder must satisfy itself that the service provider maintains robust processes and procedures regarding the relevant service (including, for example, in relation to the testing and security required in this section on Technology Governance).

81) In all circumstances, including in relation to business activities that are outsourced, an OCAB Holder is expected to maintain a strong understanding of the third party service being provided and, for critical services, have redundancy measures in place where appropriate.

82) Public and private cloud service providers should be subject to thorough screening. A set of well-defined and documented access management procedures should be in place. All service level agreements should be reviewed annually for serviceability and security of the systems and related operations as per the IT policies of the OCAB Holder. A ‘clear roles and responsibilities matrix’ should be in place to delineate operations of a service provider from those of an OCAB Holder. Physical access to systems should be limited to the relevant personnel and access should be monitored by the OCAB Holder on an ongoing basis.

83) OCAB Holders are required to retain and be in the position to retrieve the data held on a cloud platform for such duration as they are required to under ADGM/FSRA record
keeping purposes, and submit the data held on a cloud platform to the FSRA, as and when directed to do so, with immediate effect.

84) OCAB Holders who employ cloud based data storage services for the purpose of recording personal data must also take into consideration ADGM data protection regulations. Consideration must be given to the jurisdiction within which the cloud storage service provider is located, or alternatively other arrangements which may facilitate compliance with applicable data protection requirements.

Forks

85) OCAB Holders should ensure that changes in the underlying protocol of a Crypto Asset that result in a fork are managed and tested proactively. This includes temporary forks which should be managed for reverse compatibility for as long as required.

86) OCAB Holders should ensure that their Clients are able to deposit and withdraw Accepted Crypto Assets in and out of OCAB Holders’ infrastructure as and when requested before and after a fork (except during go-live). Clients should be notified well in advance of any periods of time when deposits and withdrawals are not feasible.

87) Where the underlying protocol of a Crypto Asset (e.g., the native token of that protocol) is changed, and the new version of that Crypto Asset is backwards-compatible with the old version (soft fork), OCAB Holders should ensure that the new and old versions of the Crypto Asset continue to satisfy the relevant Accepted Crypto Asset requirements.

88) Where the underlying protocol of an Accepted Crypto Asset is changed, and the older version of the Accepted Crypto Asset is no longer compatible with the new version and/or there is an entirely new and separate version of the Crypto Asset (hard fork), OCAB Holders should ensure that client balances on the old version are reconciled with the new version of the Crypto Asset. OCAB Holders should also maintain transparent lines of communication with their Clients on how OCAB Holders are managing Clients’ Crypto Asset holdings in such a scenario.

89) In the case of a hard fork, OCAB Holders should proactively manage any discrepancy between the balances recorded on the previous version versus the new version by engaging with the community which is responsible for updating and supporting the underlying protocol of the relevant Crypto Asset. Additionally, OCAB Holders should ensure that, where they seek to offer services in relation to the Crypto Asset associated with the new version of the underlying protocol, this new Crypto Asset meets the requirements for an Accepted Crypto Asset and that they notify the FSRA well in advance of offering the Crypto Asset as part of its OCAB activities.

Crypto Asset Risk Disclosures

90) Given the significant risks to Clients transacting in Crypto Assets, OCAB Holders are required to have processes in place that enable them to disclose, prior to entering into
an initial transaction, all material risks to their Clients in a manner that is clear, fair and not misleading.

91) COBS Rule 17.6 sets out a non-exhaustive list of risks that are required to be disclosed to Clients. The FSRA is of the view that merely restating this non-exhaustive list of risks, either in its application or in the risk disclosures to its Clients, does not satisfy an OCAB Holder’s risk disclosure requirements. Instead, OCAB Holders are expected to undertake a detailed analysis of the risks, and to make all necessary disclosures to their Clients. As this disclosure obligation is ongoing, and given the rapidly developing market for Crypto Assets, OCAB Holders are required to continually update this analysis and the resultant disclosures to its Clients to reflect any updated risks relating to:

a) the OCAB Holder’s products, services and activities;\(^{22}\)

b) Crypto Assets generally; and

c) the specific Accepted Crypto Asset.

92) For the purposes of interpreting the reference to “initial Transaction” in COBS Rule 17.6, OCAB Holders can meet the obligation in this Rule at any time prior to the ‘initial Transaction’. For example, the introduction of a new Accepted Crypto Currency to trading on a Crypto Asset Exchange may require a further specific risk disclosure being made to Clients of the Crypto Asset Exchange in relation to the risks of trading in that new Accepted Crypto Asset (as assessed by the Crypto Asset Exchange).

93) The FSRA will need to understand the process by which an OCAB Holder will communicate the risks outlined in COBS Rule 17.6.2, as well as any other relevant material risks to its Clients. Where the Clients of an OCAB Holder are required to enter into a Client Agreement, the OCAB Holder may make its first such risk disclosure in that Client Agreement.

94) Considering the heightened inherent risks associated with investing in Crypto Assets and the FSRA’s objective of providing a regulatory regime that offers adequate consumer protection, the FSRA is of the view that all OCAB Holders should, prior to on-boarding a Client, ensure that the services, or new services, proposed to be provided to a Client are appropriate, taking into account such matters as the Client’s relevant knowledge, experience and investment objectives. Where a conflict between the inherent risks and the appropriateness for a Client is identified, the OCAB Holder should take all reasonable steps to resolve such a conflict.

\(^{22}\) These disclosures should cover any specific arrangements, or lack of arrangements, for any product, service and activity of an OCAB Holder. For example, in relation to custody of Client’s Crypto Assets, where an OCAB Holder allows/requires Clients to self-custodise their Crypto Assets, this must be fully disclosed to Clients upfront, and Clients must be informed that the OCAB Holder is not responsible for custody and protection of Clients’ Crypto Assets. Where an OCAB Holder is outsourcing part or all of the custody arrangements to a third party, this should also be disclosed to Clients.
***Market Abuse, Transaction Reporting and Misleading Impressions (FSMR)***

95) As the OCAB Framework does not treat Crypto Assets as Financial Instruments / Specified Investments, certain FSMR provisions have been expanded to specifically capture Crypto Asset activities within ADGM.

96) Importantly, the Market Abuse Provisions in Part 8 of FSMR specifically cover Market Abuse Behaviour in relation to Accepted Crypto Assets admitted to trading on a Crypto Asset Exchange. In this regard, the FSRA imposes the same high regulatory standards to Crypto Assets traded on Crypto Asset Exchanges as it does to Financial Instruments traded on Recognised Investment Exchanges, MTFs or OTFs in ADGM.

97) Similar to the reporting requirements imposed on Recognised Investment Exchanges and MTFs, Crypto Asset Exchanges (pursuant to FSMR Section 149) are required to report details of transactions in Accepted Crypto Assets traded on their platforms. The FSRA expects Crypto Asset Exchanges to report to the FSRA on both a real-time and batch basis.

98) In addition, the FSMR provisions on Misleading Statements apply to Accepted Crypto Assets. The FSRA expects that all communications (including advertising or investment materials or other publications) made by an Authorised Person (including an OCAB Holder) will be made in an appropriate manner and that an Authorised Person (including an OCAB Holder) will implement suitable policies and procedures to comply with the requirements of FSMR.

99) The FSRA continues to consider developments to its regulatory perimeter in the context of its Market Abuse provisions, including for the purposes of any future determination of whether the provisions ought to be extended to further capture Crypto Asset trading activity that is not specifically linked to trading on a Crypto Asset Exchange. In this context, and particularly in the case of intermediary OCAB Holders, the FSRA reminds OCAB Holders of their wider responsibilities under the OCAB Framework, including in relation to client risk disclosures, suitability and best execution (see paragraphs 90-94, 100(a) and (b) and 106).

**SPECIFIC FSRA GUIDANCE ON THE OCAB FRAMEWORK**

***Application of particular Rules in COBS***

100) For the purposes of the OCAB framework and OCAB Holders, the Rules referenced in COBS 17.1.4 apply to all transactions undertaken by an OCAB Holder. The Rules referenced in COBS 17.1.4 are as follows:

a) COBS Rule 3.4 (Suitability);

---

23 The additional obligation of a Crypto Asset Exchange to undertake its own market surveillance is set out later in paragraph 127(d) of this Guidance.

24 This is particularly relevant when OCAB Holders trade into other unregulated/lightly regulated markets globally. FSRA expects OCAB Holders to have suitable controls (including client protection controls and disclosure mechanisms) in place for such activity.
b) COBS Rule 6.5 (Best Execution);

c) COBS Rule 6.7 (Aggregation and Allocation);

d) COBS Rule 6.10 (Confirmation Notes);

e) COBS Rule 6.11 (Periodic Statements); and

f) COBS Chapter 12 (Key Information and Client Agreement)).

101) These requirements are relevant to the concept of ‘Investment Business’ within COBS, and can be considered more relevant to certain OCAB Holders, particularly those that are ‘dealing’ in Accepted Crypto Assets. The FSRA understands that some of these obligations may not apply to all OCAB Holders (particularly Crypto Asset Exchanges).

102) For the avoidance of doubt all OCAB Holders that hold or control:

a) Client Money (e.g., fiat currencies) on behalf of Clients are required to comply with all relevant Client Money rules in Chapter 14 of COBS (read together with COBS Rule 17.8) at all times; and

b) Accepted Crypto Assets are required to comply with all relevant Safe Custody rules in Chapter 15 of COBS (read together with COBS Rule 17.8) at all times.

Substance requirements of OCAB Holders

103) In order to operate effectively as an OCAB Holder within ADGM, an OCAB Holder must commit resources of a nature allowing it to be operating in substance within ADGM. Depending on the relevant OCAB activity being undertaken, the FSRA expects to see substantive resources committed within ADGM across all lines of the OCAB Holder’s activity, including, but not limited to, commercial, governance, compliance/surveillance, operations, technical, IT and HR functions. The FSRA expects the ‘mind and management’ of an OCAB Holder to be located within ADGM. Further discussion on substance in relation to Crypto Asset Exchanges is set out at paragraph 123.

Crypto Asset Brokers or Dealers

104) OCAB Holders intending to operate solely as a broker or dealer for Clients (including the operation of an OTC broking or dealing desk) are not permitted to structure their broking / dealing service or platform in such a way that would have it be considered as operating a market / Crypto Asset Exchange. The FSRA would consider features such as allowing for price discovery, displaying a public trading order book (accessible to any member of the public, regardless of whether they are Clients), and allowing trades to automatically be matched using an exchange-type matching engine as characteristic of a Crypto Asset Exchange, and not activities acceptable for an OCAB intermediary to undertake.
An OCAB Holder that only has an FSP to operate as a Crypto Asset broker / dealer and not as a Crypto Asset Exchange is required to design and structure its operations, user interface, website, marketing materials and any public or client-facing information such that it does not create the impression that it is running a Crypto Asset Exchange. In practice, this may include not displaying any publicly-accessible information that may appear like a trading order book, not providing for any price discovery, and not giving actual or potential Clients the impression that they are interacting with a Crypto Asset Exchange.

Crypto Asset brokers / dealers are required to comply with the best execution requirements in COBS 6.5 at all times.

Crypto Asset brokers / dealers are required to disclose the following information to clients:

a. how they execute and route Client’s orders and source liquidity (e.g., whether they pass or route orders to other brokers, dealers or exchanges to execute). Where a Crypto Asset broker / dealer routes Client orders to a single liquidity source such as a Crypto Asset exchange for execution, it must also disclose this to all Clients;

b. whether it may carry out proprietary trading on its own account, and if so, whether it may trade against Clients’ positions;

c. the fees it charges Clients; and

d. how it determines the prices of the Accepted Crypto Assets it quotes to Clients.

Appointment of advisers

OCAB Applicants should consider the appointment of compliance advisers, with the appropriate skills, knowledge and experience (taking into account the Crypto Asset activities that the Applicant is proposing to undertake), to provide the requisite assistance to the Applicant throughout the Application process. The FSRA expects that Applicants should engage its compliance advisers by no later than when it begins to prepare its Application, and should retain them up until the date of operational launch.

Certain class order modifications / waivers

The FSRA appreciates that some Rules, in particular within MIR and parts of COBS, may not apply to certain OCAB Holders and the FSRA may grant class order modification and waiver relief in relation to these Rules. To the extent that an Applicant or OCAB Holder considers that any other Rules do not apply to it by virtue of its business model or otherwise, the FSRA expects that an application for modification or relief be

25 Unless they also hold an FSP that allows them to operate as a Crypto Asset Exchange.
26 The FSRA would not allow Crypto Asset brokers / dealers to “front run” or trade ahead of Clients’ trades, or trade on a proprietary basis alongside Clients’ trades.
27 Any such relief, and the terms on which it is based, is located at http://adgm.complinet.com/net_file_store/new_rulebooks/c/l/ClassModification_Notice_Authorised_Persons_undertaking_Regulated_Activity_of_OCAB_13_May_2019.pdf
submitted either as part of its OCAB Application or at such later date as the relief may be required.

Data protection obligations for OCAB Holders

110) ADGM’s data protection regime protects individuals’ right to privacy by controlling how personal information is used by organisations and businesses registered in ADGM. All entities registered in ADGM that hold or process the personal data of an individual must protect personal data in compliance with the ADGM Data Protection Regulations 2015 (the “Data Protection Regulations”). Specifically, an OCAB Holder, as a data controller, will be responsible for determining the purposes for which, and the manner in which, personal data is processed in compliance with the Data Protection Regulations. Failure to do so risks enforcement action and compensation claims from individuals, each of which are considered data subjects under the Data Protection Regulations.

111) Data controllers must ensure that personal data which they process is:

   a) processed fairly, lawfully and securely;

   b) processed for specified, explicit and legitimate purposes in accordance with the data subject's rights and not further processed in a way incompatible with those purposes or rights;

   c) adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed;

   d) accurate and, where necessary, kept up to date; and

   e) kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data were collected or for which they are further processed.

112) Data controllers must, on request, provide individuals with access to any personal information they hold.

113) The registration of all data controllers with the ADGM’s Registration Authority\textsuperscript{28} is mandatory. A data controller must maintain records of all personal data processing operations undertaken by it or on its behalf and must notify the Registration Authority upon becoming aware of any security breach involving personal data as soon as possible.

\textsuperscript{28} Detailed information concerning data protection obligations under the ADGM data protection regime, including registration forms, fee information and specific guidance is available on the Registration Authority website.
114) Personal data must not be transferred to a country or territory outside ADGM unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The Registration Authority has designated certain jurisdictions as providing an adequate level of protection; a current list is maintained by the Registration Authority upon its website, which may be updated from time to time.

115) If an OCAB Holder intends to transfer personal data to a recipient, including by way of storage of personal information upon a cloud based service or remote server, located in a jurisdiction other than those considered by the Registration Authority to be possessing adequate safeguards, such transfer is only possible under certain conditions, including, but not limited to, circumstances where the:

a) individual has consented to the proposed transfer;

b) proposed transfer is necessary for the performance of the service for which the data controller was engaged by the individual; and

c) data controller and data processor have entered into an approved form of agreement concerning the protection of personal data, or the Registration Authority has granted a permit consenting to the proposed transfer.

Transactions with unknown counterparties

116) OCAB Holders should avoid transactional interaction with any infrastructure or services where a counterparty is unknown or anonymous (e.g., via certain peer to peer or decentralised exchanges) at any stage of the process within and outside of the OCAB Holders’ core operations. This is to ensure that OCAB Holders remain compliant with FSRA Rules at all times and do not unnecessarily expose their OCAB activities to risks emanating from tainted sources / destination of funds.

117) OCAB Holders should also avoid inclusion of liquidity, pricing and settlement data from such entities in their day to day operations. Any interaction (whether deliberate or not) with such entities should be notified to the FSRA as soon as practicable.

Margin trading

118) An Applicant/OCAB Holder wishing to provide margin trading to its Clients will need to submit for approval details of the terms upon which it proposes to do so (for an Applicant, in its Application – for an OCAB Holder as part of ongoing supervisory arrangements). As a general position, the FSRA would only consider allowing Applicants/OCAB Holders with relevant proven track record to provide margin trading.

119) Particular focus will be placed on an Applicant or OCAB Holder’s proposed leverage ratio. The FSRA is aware that some of the significant Crypto Asset markets around the world operate margin ratios of between 2-4 times, and it is likely that FSRA consideration of leverage ratios will be in reference to this position.
120) Applicants that are not proposing, or permitted, to carry out margin trading will have a restriction from doing so placed on their FSP.

Insurance

121) The FSRA recognises the growing interest/interplay between Crypto Asset activities and the provision of insurance to such activities. While recognising this, the FSRA does not require OCAB Holders to maintain insurance in relation to the Crypto Asset activities that they are carrying out, as the provision of insurance is considered a second line of defence. As a first line of defence, the FSRA expects all OCAB Holders to ensure the proper structuring of their business operations and to implement robust mechanisms for the mitigation of actual and potential areas of risk.

CRYPTO ASSET EXCHANGES

Background

122) Whilst multiple Crypto Asset activities can be conducted and regulated by the FSRA within ADGM, as set out in section 73B of Schedule 1 of FSMR, the FSRA considers the Crypto Asset activities undertaken by Crypto Asset Exchanges to be a key Crypto Asset activity in ADGM. For this reason, the OCAB Framework contains specific additional requirements applicable to Crypto Asset Exchanges. The approach taken by the FSRA to the regulation of Crypto Asset Exchanges is to treat them similarly to Multilateral Trading Facilities (“MTFs”).

Substance requirements for Crypto Asset Exchanges

123) Consistent with the treatment of all OCAB Holders (see paragraph 103), the FSRA considers that operating a Crypto Asset Exchange within ADGM requires the Crypto Asset Exchange to be based in substance within ADGM. In addition to the substantial commitment of resources required of an OCAB Holder, this also means that the FSRA’s regulatory oversight of a Crypto Asset Exchange extends to its order book, matching engine, rulebook(s), ensuring fair and orderly markets, settlement, and for the purposes of preventing/monitoring for Market Abuse, amongst the relevant requirements set out in the Market Infrastructure Rules (“MIR”) and COBS Chapter 8.

124) In practical terms, this means that for a start-up Crypto Asset Exchange, its entire order book and the functionality of its matching engine will be subject to FSRA oversight. For existing operational crypto asset exchanges that already have their order book / matching engine outside ADGM prior to making an application, a determination of which parts (if not all) of its order book (and how its matching engine) will come under FSRA regulatory oversight needs to be made by the Applicant, 29 to allow it to apply to become authorised as a Crypto Asset Exchange.

29 In situations where an entity establishes an OCAB Holder that routes orders to a crypto asset exchange outside ADGM (even as part of a Group that may be operating globally) instead of having orders matched within an exchange’s order book within ADGM, that entity cannot obtain a Crypto Asset Exchange license within ADGM and can only be licensed as a general OCAB Holder within ADGM.
125) The FSRA is of the view that only Crypto Asset Exchanges can operate markets within ADGM that allow for the matching of orders, or for the purposes of price discovery, of Accepted Crypto Assets. For this reason, and the reasons set out above, the application of FSRA’s regulatory oversight may, therefore, be distinctly different from other regulators globally.

**Guidance in relation to Applicable Rules**

126) In addition to the requirements set out in COBS Rules 17.1 to 17.6, Crypto Asset Exchanges are also required to meet the additional Rules set out in COBS 17.7. COBS Rule 17.7.2 requires that a Crypto Asset Exchange comply with the requirements set out in Chapter 8 of COBS, being the principal Rules relevant to the operation of an MTF. 30

127) Chapter 8 of COBS incorporates Rules from various other FSRA Rulebooks that must be complied with, including certain sections of MIR. COBS Rule 8.2.1 sets out various Rules in MIR that OCAB Holders are required to comply with to the satisfaction of the FSRA, with the applicable Rules set out as follows:

a) Mir Rule 2.6 (Operational systems and controls): Mir Rule 2.6.1 requires a Crypto Asset Exchange to ‘establish a robust operational risk management framework with appropriate systems and controls to identify, monitor and manage operational risks that key participants, other [Crypto Asset Exchanges], service providers (including outsourcees) and utility providers might pose to itself.’

i. In considering systems and controls, the FSRA has provided guidance on what it expects in relation to Technology governance controls in paragraphs 45 to 89 of this Guidance, such that the FSRA’s expectations in this area are similar to what is expected of Recognised Investment Exchanges or MTFs generally. The FSRA therefore requires a Crypto Asset Exchange to undertake its ‘exchange-type’ activities in compliance with these operational system and control requirements, in combination with the Technology governance controls outlined earlier in this Guidance.

ii. The FSRA expects a Crypto Asset Exchange to undertake extensive due diligence and testing of its operational system and controls, with the relevant reports of such testing capable of being provided to the FSRA for review. Such testing should be undertaken by an officer of the Crypto Asset Exchange possessing appropriate skills and experience. The testing reports need to confirm the robustness of the Crypto Asset Exchange’s systems, and address any potential areas of failure. Testing should include the settlement processes for the movement of Crypto Assets between wallets, and the general connectivity of the Crypto Asset Exchange’s systems with other parties. Testing

---

30 Chapter 8 of COBS also contains the requirements for the operation of an Organised Trading Facility (OTFs). The application of OTF Rules, however, are not relevant to the operation of a Crypto Asset Exchange.
should be ongoing, building in processes for the introduction of new Accepted Crypto Assets.

iii. A Crypto Asset Exchange will need to provide policies and procedures that clearly evidence how it will effectively address a failure of its systems. Failures must be rectified as soon as practicable, with a Crypto Asset Exchange’s business continuity plan including detailed and realistic response timeframes for failures or disruptions.

b) MIR Rules 2.7.1 and 2.7.2 (Transaction recording): FSRA expects that the primary ledger technology systems and controls of a Crypto Asset Exchange (whether they be DLT or multiple-ledger technologies) will be such that transaction recording and reporting is easily facilitated, and that all FSRA requirements can be effectively complied with. Where reconciliations are required to be undertaken, for example, between a DLT based ledger and an internal ledger maintained by a Crypto Asset Exchange for the purposes of transactions and/or settlement, the FSRA will need to be satisfied that the reconciliation process is robust, timely and efficient.

c) MIR Rule 2.8 (Membership criteria and access): MIR Rule 2.8.1 requires that a Crypto Asset Exchange ‘must ensure that access to its facilities is subject to criteria designed to protect the orderly functioning of the market and the interests of investors’.

Access Requirements

i. MIR Rules 2.8.2, 2.8.3, 2.8.5 and 2.8.6 support the operation of MIR Rule 2.8.1, and the FSRA expects that Crypto Asset Exchanges consider the application of the requirements across these Rules - for example, MIR Rule 2.8.5 contains substantive provisions that should apply, regardless of what model of ‘access’ a Crypto Asset Exchange utilises.

ii. The FSRA recognises, however, that Crypto Asset Exchanges generally operate an ‘access’ model that does not include Members31 (e.g., access is granted directly to (retail and institutional) Clients of a Crypto Asset Exchange). A Crypto Asset Exchange will, therefore, need to ensure that it has appropriate processes, controls and rules to ‘protect the orderly functioning’ of its market, its facilities and the interests of its investors.

iii. By not adopting a ‘Member-access’ model and allowing direct ‘Client-access’, Crypto Asset Exchanges lose one layer of regulatory/supervisory defense that Recognised Investment Exchanges and MTFs have, in that they do not have Members assisting them in the undertaking of the necessary due diligence and compliance reviews of investors being onboarded into their market. The FSRA, in these circumstances, requires Crypto Asset Exchanges to undertake their own CDD reviews for every client accessing (trading on) their market.

31 To clarify, ‘Members’ are not the same as ‘Institutional Clients’.
(something which traditionally a Recognised Investment Exchange or MTF can rely on its Members to do). Resultant AML/CFT obligations therefore fall more directly on a Crypto Asset Exchange as well.

iv. The FSRA expects that the controls (and resultant resourcing needs) of a Crypto Asset Exchange be appropriately budgeted and accounted for, including specific controls for when it has Clients that are institutional Clients (as the current conventional Member/institutional client global regulatory model may not properly account for, and mitigate, the risks relevant to operating such model within the Crypto Asset space). For example, where a Crypto Asset Exchange has institutional Clients that are regulated as OCAB Holders (for example, an OCAB Holder that is a broker / dealer) within ADGM, the Crypto Asset Exchange may take comfort from the fact that its Clients are appropriately regulated (including for AML purposes). A Crypto Asset Exchange may not, however, take such comfort when its institutional Clients may come from unregulated/less regulated jurisdictions. Crypto Asset Exchanges with an institutional Client base will therefore need to demonstrate how the Crypto Asset Exchange will adequately comply with the requirements of the AML Rulebook where its institutional Clients are trading on behalf of further clients.

v. Given the current lack of global regulation of Crypto Asset intermediaries, those Crypto Asset Exchanges operating a ‘membership model’ will need to assess whether their members are adequately regulated in their home jurisdiction, such that the Crypto Asset Exchanges can suitably rely on their Members, for example, to undertake CDD/AML checks. Where members are not properly regulated, the FSRA expects that Crypto Asset Exchanges will centralise the relevant compliance activities internally (and not be able to rely on their ‘members’ for such purposes).

vi. Depending on the model, controls and criteria to be adopted by a Crypto Asset Exchange, the class order modification or waiver relief granted by the FSRA to OCAB Holders as referred to in paragraph 109 of the Guidance may apply.

**Rulebook(s)**

vii. Further to MIR Rule 2.8, the FSRA expects a Crypto Asset Exchange to have a rulebook(s) in place. This rulebook should be clearly labelled as such, and be publicly available on the website of the Crypto Asset Exchange.

viii. Supporting documents such as participation agreements, terms of business, product lists, user guides and technical specifications are also a key part of the operation of a Crypto Asset Exchange, and should be consistent with its rulebook. The FSRA does not consider that the existence of these documents alone meet the requirement of having a transparent and effective rulebook. The FSRA considers it good practice that these supporting documents are
available and transparent, alongside the published rulebook, to the extent possible.

ix. The content of a rulebook\textsuperscript{32} should enable a Crypto Asset Exchange to demonstrate how it is complying with MIR Rule 2.8, be supported by procedures that are complete and clear, and all in support of a Crypto Asset Exchange seeking to ensure that behaviour within its market is fair and orderly.

x. The FSRA expects Crypto Asset Exchanges to require explicit acknowledgement via a user agreement, that participants have read, understood and will abide by the rulebook at all times.

xi. The FSRA expects a Crypto Asset Exchange to undertake regular reviews of its rulebook to ensure it is consistent with relevant regulatory and legislative requirements. Best practice may see such activity undertaken no less than every twelve-months.

d) MIR Rule 2.9 (Financial crime and market abuse): Crypto Asset Exchanges are required to operate an effective market surveillance program to identify, monitor, detect and prevent conduct amounting to market misconduct and/or Financial Crime. Given the significant risks, and the nascent nature and constant pace of development of the Crypto Asset industry, a Crypto Asset Exchange’s surveillance system will need to be robust, and regularly reviewed and enhanced.

i. The FSRA recognises that Crypto Asset Exchanges outside ADGM may not be subject to a similar regulatory standard as that which applies within ADGM. The FSRA recommends, therefore, that Crypto Asset Exchanges spend the time to consider the application of MIR Rules 2.9.1 to 2.9.3, which technology, systems and controls they propose to use for these purposes, and the

\textsuperscript{32} A non-exhaustive list of sections that the FSRA consider key for inclusion in a rulebook include:

- participant eligibility criteria;
- participant obligations;
- Accepted Crypto Asset eligibility criteria;
- Crypto Asset fork protocols;
- fair and orderly trading rules;
- AML and source of fund requirements;
- market abuse prohibition rules;
- measures to prevent a disorderly market;
- disciplinary procedures;
- pre- and post-trade obligations;
- settlement obligations;
- certain wallet and custody provisions;
- default provisions;
- compliance;
- monitoring & enforcement;
- definitions / glossary of terms;
- co-operation with regulators; and
- powers to amend rules and consultation procedures.
associated resourcing needs required to undertake these functions appropriately. For this reason, among others set out in this Guidance, the FSRA is of the view that it is not appropriate for a Crypto Asset Exchange to outsource its compliance / market surveillance functions.

ii. The FSRA further reminds Crypto Asset Exchanges, and investors trading on a Crypto Asset Exchange, of the Market Abuse provisions applicable to the trading of Accepted Crypto Assets on a Crypto Asset Exchange.33

e) MIR Rule 2.11 (Rules and consultation): To meet MIR Rules 2.11.1 to 2.11.11, a Crypto Asset Exchange must ensure that it has appropriate procedures in place for it to make rules, for keeping its rules under review, for consulting and for amending its rules. MIR Rule 2.11.2 requires proposed rule changes be subject to FSRA approval.

f) MIR Rule 3.3 (Fair and orderly trading): MIR Rules 3.3.1 to 3.3.4 establish the requirements a Crypto Asset Exchange must meet for providing fair and orderly trading across its market, and for having objective criteria for the efficient execution of orders. The FSRA considers these requirements to be fundamental to the operation of a Crypto Asset Exchange.

g) COBS Rule 8.3.1 & MIR Rule 3.7 (Public disclosure):

i. Any arrangements of a Crypto Asset Exchange used to make information public (including trading information required to be disclosed under COBS Rule 8.3.1) must satisfy a number of conditions, including that it is reliable, monitored continuously, and made available to the public on a non-discriminatory basis. While a Crypto Asset Exchange can choose the format structure to be used for dissemination, MIR Rule 3.7.4 requires it to conform to a consistent and structured format.

ii. In terms of the timing of disclosure of Crypto Asset Exchange trading information, the FSRA recognises that current crypto asset industry practice is for such trading information to be released on a real-time basis (in alignment with current practice for trading within spot commodity markets, but different to the current industry/regulatory practice of delayed data within certain securities/derivatives markets). The FSRA is not proposing any additional specific requirements at this stage (to those already applicable in COBS Rule 8.3.1 and MIR Rule 3.7), but will continue to monitor industry practice.

h) MIR Rule 3.8 (Settlement and Clearing Services): A Crypto Asset Exchange will need to have clear processes in place for the settlement (and if applicable, the clearing) of all Accepted Crypto Asset transactions. As noted in the AML and Technology Governance sections of this Guidance, extensive stress testing on capabilities to connect successfully with third parties, and in relation to the movement of

33 Refer to paragraphs 95 to 99 of this Guidance.
Accepted Crypto Assets between wallets, will be required to be undertaken to the FSRA’s satisfaction. The FSRA will not necessarily require a connection to a separate Recognised (or Remote) Clearing House where the Crypto Asset Exchange can demonstrate that it has in place ‘satisfactory arrangements for the timely discharge, Clearing and settlement of the rights and liabilities of the parties to transactions effected’ on the Crypto Asset Exchange, including where it is utilising the services of ADGM-regulated Crypto Asset Custodian.

i) MIR Rule 3.10 (Default Rules): Depending on whether a Crypto Asset Exchange operates a ‘Member-access’ model or it allows direct ‘Client-access’ will determine the full, or partial, application of MIR Rules 3.10.1 to 3.10.3. The FSRA, at a minimum, expects Crypto Asset Exchanges to have in place both rules and a process to suspend or terminate access to its markets in circumstances where a Client/Member is unable to meet its obligations in respect of transactions relating to Accepted Crypto Assets.

i. The FSRA suggests that an Applicant/OCAB Holder consider different scenarios/circumstances where it may need to utilise the powers provided to it under its Default Rules, and take appropriate action as required. Scenario testing of this kind could relate to when there is a financial and/or technical ‘default’ in relation to, for example, its custody, fiat token or wider banking arrangements. Due to a prevalence of pre-funding of (client) positions within OCAB markets, the impact of a ‘default’ in such a scenario may not necessarily be on a per-transaction basis, but could be structural in nature, in limiting the ability of Clients to fund their positions (and therefore the ability of the Crypto Asset Exchange to operate on a fair and orderly basis).

ii. To prepare for the event of a loss/default, the FSRA expects a Crypto Asset Exchange to have, within its policies, a clear process for the management of such loss (e.g., what is the exposure of individual Clients, counterparties, its Crypto Asset Custodian and itself, as applicable).

128) COBS Rule 17.7.4 specifies that certain notification requirements applicable to Recognised Investment Exchanges under MIR Rules 5.1, 5.3 and certain information requirements under MIR Rule 5.4.1 apply to Crypto Asset Exchanges. These are specific requirements applicable to Crypto Asset Exchanges that are not applied to MTFs. Crypto Asset Exchanges will also need to comply with any other applicable notification requirements, including those set out in paragraph 29 of this Guidance in relation to the use of additional Accepted Crypto Assets.

129) It is recognised that Crypto Asset Exchanges may take varying approaches in relation to the custody of fiat currencies and Crypto Assets. A Crypto Asset Exchange may use third party custodians but still be holding itself out to its Clients as being responsible for custody of their fiat currencies and Accepted Crypto Assets. Alternatively, a Crypto Asset Exchange may provide custody of Clients’ fiat currencies and Accepted Crypto Assets wholly itself, done “in-house” without the use of any third party custodians. A Crypto Asset Exchange whose custody arrangements fall into either of these two
scenarios will also be considered to be Operating as a Crypto Asset Custodian for the purposes of this framework, and will be required to comply with COBS Rule 17.8, and take guidance from the sections below on “Crypto Asset Custodians”.

130) As further set out in paragraphs 150 and 151, in circumstances where a Crypto Asset Exchange operates as a Crypto Asset Custodian, the FSRA expects appropriate segregation of responsibilities, staff, technology and, as appropriate, financial resources, between the operations of a Crypto Asset Exchange and the Crypto Asset Custodian.

**Recognised Investment Exchanges Operating a Crypto Asset Exchange**

131) Pursuant to MIR Rule 3.4.1A, a Recognised Investment Exchange may operate a Crypto Asset Exchange, as part of the Regulated Activity of Operating a Crypto Asset Business, provided that its Recognition Order includes a stipulation permitting it to do so. MIR Rule 3.4.2 requires that where such a stipulation is granted to a Recognised Investment Exchange, the Recognised Investment Exchange must meet the requirements of the OCAB Framework in relation to operation of the Crypto Asset Exchange while the remainder of its operations must be operated in compliance with the MIR Rules.

132) This means that a Recognised Investment Exchange (in addition to operating markets relating to the trading of Financial Instruments (including Digital Securities) can, where permitted by the FSRA and subject to MIR Rule 3.4.2, operate a separate MTF, OTF and/or Crypto Asset Exchange under its Recognition Order.

133) OCAB Holders that are operating a Crypto Asset Exchange wishing to also operate a Recognised Investment Exchange will be required to relinquish their FSP upon obtaining a Recognition Order (to operate a Recognised Investment Exchange). If licensed by the FSRA to carry out both Regulated Activities (e.g., operating a Crypto Asset Exchange and operating a Recognised Investment Exchange), the Recognition Order will include a stipulation to that effect pursuant to MIR Rule 3.4.1A - see paragraph 131 above).

134) The FSRA appreciates that Applicants, OCAB Holders and Recognised Bodies may wish to build out their Regulated Activities in ADGM on a staggered basis. For example, an entity may wish to start out in ADGM as a Crypto Asset Exchange and migrate to other exchange/market infrastructure activities in due course. Equally, a Recognised Investment Exchange may wish to start out in the area of Derivatives or Digital Securities, and then introduce Crypto Asset Exchange activities in due course. The FSRA suggests that in such circumstances an Applicant reach out to discuss the steps for doing so as early as possible.

**CRYPTO ASSET CUSTODIANS**

135) Crypto Asset Custodians provide the service of helping Clients safeguard their Accepted Crypto Assets. Some Crypto Asset Custodians may also, in addition, help
Clients safeguard their fiat currencies (referred to as “Client Money”)\(^{34}\). Crypto Asset Custodians include firms that solely offer the custody of Crypto Assets and / or Client Money for Clients, as well as Crypto Asset Exchanges and OCAB intermediaries who additionally provide the service of custodising Accepted Crypto Assets or Client Money on behalf of Clients.

136) Similar to the approach taken in relation to Crypto Asset activities undertaken by Crypto Asset Exchanges, the FSRA considers the Crypto Asset activities undertaken by Crypto Asset Custodians to be a key Crypto Asset activity within ADGM. Accordingly, the OCAB Framework contains specific additional requirements applicable to Crypto Asset Custodians.

137) In addition to having to meet the requirements set out in COBS Rules 17.1 to 17.6, Crypto Asset Custodians are required to meet the additional Rules set out in COBS 17.8. For the purposes of Operating a Crypto Asset Business, COBS Rule 17.8.2 requires that the existing definitions of “Providing Custody”, “Client Assets” and “Client Investments” be read to include “Crypto Assets” and that “Investment Business” be read to include a “Crypto Asset Business”. This approach has been taken by the FSRA to ensure that Accepted Crypto Assets are afforded the same protections as other similar products and activities under FSMR and the FSRA Rulebook.

**Protection of Client Money**

138) As noted earlier in paragraph 102, Chapter 14 of COBS sets out various requirements that Authorised Persons, including OCAB Holders, must comply with to ensure that they properly protect and safeguard any Client Money that they are holding or controlling on behalf of their Clients. COBS Rule 17.8 further clarifies these requirements in relation to Crypto Asset Custodians that are holding or controlling Client Money.

139) “Client Money” refers to money (e.g., fiat) of any currency which an Authorised Person holds on behalf of a Client or which an Authorised Person treats as Client Money, subject to the exclusions in COBS 14.2.6. In carrying out their activities, OCAB Holders may at certain junctures be holding or controlling Client Money when providing Crypto Asset-related products and services to their Clients.

140) The following are examples of situations where an OCAB Holder would be considered to be holding or controlling Client Money:

   a) **Example 1**: To fund their trading account at a Crypto Asset Exchange, a Client of the Crypto Asset Exchange transfers US dollars (in fiat) from their bank account to their account at the Crypto Asset Exchange. These US dollars held by the Crypto Asset Exchange for the Client - before they are used to purchase any Accepted Crypto Assets - would be considered Client Money.

---

\(^{34}\) Crypto Asset Custodians that custodise fiat currencies for clients would be expected to hold the fiat currency with a regulated bank in a Client Money Account operated under the instructions of the Crypto Asset Custodian.
b) **Example 2**: A Client of a Crypto Asset Exchange holds bitcoins in their wallet at a Crypto Asset Exchange. They use the Crypto Asset Exchange to sell their bitcoins in exchange for US dollars (in fiat). The US dollars are then credited to their account at the Crypto Asset Exchange and held by the Crypto Asset Exchange for them. These US dollars held in their account with the Crypto Asset Exchange would be considered Client Money.

c) **Example 3**: A fully fiat-backed stablecoin\(^{35}\) issuer accepts fiat from Clients in exchange for giving them stablecoins. The fiat currency held by the issuer would be considered as Client Money (and which can be redeemed by Clients on presentation of the stablecoin), and the fiat-backed stablecoin issuer would need to comply with the Client Money provisions in COBS.

141) A Crypto Asset Custodian that holds or controls Client Money must comply with all the relevant Client Money rules in Chapter 14 of COBS (read together with COBS Rule 17.8) at all times.\(^{36}\) In particular, such Crypto Asset Custodians are required to carry out reconciliations of Client Money in Client Accounts as follows:

a) Reconciliations with respect to COBS Rule 14.2.12(a) shall be carried out at least every week; and

b) Reconciliations with respect to COBS Rule 14.2.12(d) shall be carried out within 5 days of the date to which the reconciliation relates.

**Safe Custody of Clients’ Crypto Assets**

142) The FSRA notes that there are broadly three types of custodial arrangements over Accepted Crypto Assets that OCAB Holders are likely to adopt:\(^{37}\)

a) **Type 1 (Custodial Wallet)**: The OCAB Holder is wholly responsible for the custody of a Client’s Accepted Crypto Assets and provides this service “in-house” through its own Crypto Asset wallet solution. Such an arrangement includes scenarios where a Crypto Asset Exchange provides its own in-house proprietary wallet for Clients to store any Accepted Crypto Assets bought through that exchange or transferred into the wallet from other sources. Type 1 also includes firms who solely provide the dedicated service of helping Clients (such as Crypto Asset Exchanges, broker-dealers, traders, fund / asset managers) custodize their Accepted Crypto Assets. The Type 1 custody provider effectively holds Crypto Assets (e.g., the private

---

\(^{35}\) For further details on the FSRA’s treatment of stablecoins, please refer to paragraph 155 of this Guidance.

\(^{36}\) As noted in paragraph 137, all OCAB holders holding or controlling Client Money need to comply with Chapter 14 of COBS (read together with COBS Rule 17.8) at all times.

\(^{37}\) The FSRA recognises that there may be other alternative Crypto Asset custody models in existence or which may emerge in future. Entities seeking to provide such alternative models and who are unsure of the regulatory obligations they may attract are encouraged to contact the FSRA as early as possible.
keys) as an agent on behalf of Clients, and has control over these Accepted Crypto Assets.

b) **Type 2 (Outsourced Custodial Wallet):** The OCAB Holder is wholly responsible for the custody of a Client’s Accepted Crypto Assets but operationally outsources this function to a third-party crypto asset custodian. Type 2 arrangements include the scenario where a Crypto Asset Exchange uses a third party custody service provider to hold its Clients’ Accepted Crypto Assets.

c) **Type 3 (Non-Custodial / Self-Custody Wallet):** The OCAB Holder allows/requires Clients to wholly “self-custodise” their Accepted Crypto Assets, and at no point does the OCAB Holder have partial or full control over these Clients’ Crypto Assets. The Type 3 custody provider is typically a third-party hardware or software company that offers the means for each Client to hold their Crypto Assets (and fully control private keys) themselves. Hardware wallets, mobile wallets, desktop wallets and paper wallets are generally examples of non-custodial wallets. Clients using non-custodial wallets have full control of and sole responsibility for their Crypto Assets, and the non-custodial wallet provider does not have the ability to effect unilateral transfers of Clients’ Crypto Assets without Clients’ authorisation.

Entities seeking to operate either Type 1 or Type 2 custodial arrangements above would generally be regarded as carrying out the Regulated Activity of Operating as a Crypto Asset Custodian, and require an OCAB FSP from the FSRA.

With respect to the Type 3 non-custodial wallets described above, the wallet provider is merely providing the technology; it is the wallet user himself who has full control of and responsibility for his Crypto Assets. Given they have no control over Clients’ Crypto Assets, Type 3 non-custodial wallet providers would generally not be required to seek an FSP to operate a Crypto Asset Custodian. The FSRA considers the Type 3 scenario above, where Clients are required to self-custodise their Accepted Crypto Assets, as potentially posing a material risk given that the burden of protecting and safeguarding Crypto Assets falls wholly upon Clients, and that Crypto Assets face the constant risk of being stolen by malicious actors. As such, OCAB Holders requiring Clients to self-custodise Crypto Assets are required to disclose this fact fully and clearly upfront to Clients, and meet the disclosure standards elaborated in paragraphs 90 to 94 above. The FSRA will take the quality of these proposed disclosures into account.

---

38 Clients using such Type 1 custodial wallets do not necessarily have full and sole control over their Accepted Crypto Assets. In addition, there is a risk that should the custodial wallet provider cease operations or get hacked, Clients may lose their Accepted Crypto Assets.

39 The Type 2 custody arrangement would include the scenario where an OCAB Holder engages an external third party Crypto Asset custody provider to safeguard / custodise Clients’ Accepted Crypto Assets, but the OCAB Holder is still designated as one of the multi-signature signatories required to “sign” or authorise the transfer of movement of Client’s Accepted Crypto Assets. The OCAB Holder still retains responsibility at all times to Clients for safeguarding their Accepted Crypto Assets.

40 The Type 3 custody arrangements may include scenarios where some distributed Crypto Asset Exchanges require Clients to self-custodise their Accepted Crypto Assets. Such exchanges only provide the trading platform for Clients to buy and sell Accepted Crypto Assets. Clients are required to source and use their own third party custody arrangements (which the distributed Crypto Asset Exchanges have no control over or responsibility for).
when assessing applications from OCAB Holders proposing to require Clients to self-custodise their Crypto Assets.

145) Chapter 15 of COBS sets out various requirements that all Authorised Persons, including OCAB Holders, must comply with to ensure that they properly protect and safeguard any Client Investments they are holding, controlling, providing custody for, or arranging custody for, on behalf of their Clients. Chapter 17 of COBS further describes how the Safe Custody rules in Chapter 15 apply to Crypto Asset Custodians.

146) “Client Investments” in the context of Crypto Asset Custodians refer specifically to Accepted Crypto Assets and not to money (in fiat) of any currency. Refer to paragraphs 138 to 141 above for guidance on how Crypto Asset Custodians are required to properly protect and safeguard Client Money (in fiat).

147) An OCAB Holder that holds, controls, provides custody for, or arranges custody for, with respect to Accepted Crypto Assets, on behalf of their Clients, is considered a “Crypto Asset Custodian”, and must comply with all the relevant Safe Custody rules in Chapter 15 of COBS (read together with Chapter 17 of COBS) at all times.

148) In this regard, Crypto Asset Exchanges that provide an integrated Crypto Asset wallet would need to comply with these Safe Custody rules. Crypto Asset Exchanges that outsource their Crypto Asset wallets to a third party as set out in paragraph 142(b) would also need to comply or ensure compliance with these Custody Rules, as applicable.

149) OCAB Holders operating as Crypto Asset Custodians are required, with respect to the Accepted Crypto Assets they hold under custody for Clients, to:

   a) Send out statements of a Client’s Accepted Crypto Assets holdings to Retail Clients at least monthly (as required under COBS Rule 15.8.1(a)); and

   b) Carry out all reconciliations of a Client’s Accepted Crypto Asset holdings at least every week (as required under COBS Rule 15.9.1).

**Governance Arrangements for Crypto Asset Custodians**

150) From a governance perspective, an OCAB Holder operating as a Crypto Asset Custodian should have proper governance structures in place to avoid or mitigate actual or potential conflicts of interest between its custody functions and any other activities or functions within itself or with other Group entities. Such governance arrangements may include having a separate team, which does not have other conflicting responsibilities within the firm, handling custody.

151) To assist with ring-fencing and to reduce potential conflicts of interest, an Applicant that wishes to operate as a Crypto Asset Custodian and concurrently provide other OCAB or conventional Regulated Activities should consider the merit of establishing a
separate, standalone legal entity for its Crypto Asset Custodian activities. If so established, this standalone entity would need to apply to the FSRA for its own FSP to carry on the Regulated Activity of Operating as a Crypto Asset Custodian.

Other Requirements Pertaining to Custody of Crypto Assets

Governance

152) OCAB Holders operating as Crypto Asset Custodians must not, at any time, permit arrangements whereby just a sole party or signatory is able to completely authorise the movement, transfer or withdrawal of Accepted Crypto Assets or Client Money held under custody on behalf of Clients. In particular, OCAB Holders must not have custody arrangements whereby only a sole person can fully access the private key or keys for the Accepted Crypto Assets held under custody by the OCAB Holder. Preventing such arrangements can help reduce potential key person risk such as theft, fraud, unwillingness or inability of the sole party to grant access to private keys.

153) OCAB Holders operating as Crypto Asset Custodians are also required to mitigate the risk of collusion between all authorised parties or signatories who are able to authorise the movement, transfer or withdrawal of Accepted Crypto Assets or Client Money held under custody. OCAB Holders are required to provide information on these mitigating controls to the FSRA.

154) OCAB Holders operating as Crypto Asset Custodians are required to maintain, at all times, an updated list of all past and present authorised persons who were / are able to view, initiate, authorise, sign, approve or complete the transfer or withdrawal of Accepted Crypto Assets or Client Money held under custody on behalf of Clients. In addition, OCAB Holders must have clearly defined policies and procedures to enable or revoke the authority granted to these persons.

155) OCAB Holders operating as Crypto Asset Custodians are required to have policies and procedures in place that clearly describe the process that will be adopted in the event that it knows or suspects that the Accepted Crypto Assets or Client Money it is holding under custody on behalf for Clients has been compromised, such as in the event of a hacking attack, theft or fraud. Such policies and procedures should detail the specific steps the firm will take to protect Clients’ Accepted Crypto Assets and Client Money in the event of such incidents. Crypto Asset Custodians should also have the ability to immediately halt all further transactions with regard to the Accepted Crypto Assets and Client Money.

Obligations in relation to outsourcing

156) Where an OCAB Holder that seeks to operate as a Crypto Asset Custodian wishes to outsource part or all of the custody function to a third party, the OCAB Holder is required to perform its due diligence and background checks on the third party, and

---

41 For example, a Crypto Asset Exchange may decide to offer a dedicated Accepted Crypto Asset custody service to certain Clients.
ensure that the third party meets all the FSRA’s requirements applicable to Crypto Asset Custodians. Such OCAB Holders are required to make full disclosures to their Clients and to the FSRA regarding such outsourced custody arrangements. The OCAB Holder retains full responsibility from a regulatory perspective for any issues that may result from such outsourcing, including the failure of any third party to meet its Crypto Asset Custody obligations.

*Third party audit obligations*

157) OCAB Holders should have independent third party verification or checks carried out at least annually to verify that the amount and value of Accepted Crypto Assets and Client Money (e.g., fiat) held on custody on behalf of Clients is correct and matches what the OCAB Holders are supposed to hold.

**STABLECOINS**

158) A stablecoin is a blockchain-based token that is valued by reference to an underlying fiat currency or basket of assets. A key feature of a stablecoin is that it purports to have less volatility than other Crypto Assets, allowing it to operate as a transfer of value within the Crypto Asset ecosystem, including as one leg of a trading pair on Crypto Asset Exchanges. Demand continues to grow for effective stablecoins within Crypto Asset markets as many participants seek a safe store of value (in terms of reconciliation and to protect from manipulation). Demand has also increased as a result of the general inability to liquidate Crypto Assets into fiat currencies. Additionally, some stablecoins are aimed more as operating as a ‘digital currency’ within the digital economy.

159) Various stablecoin issuers have entered the Crypto Asset ecosystem, with a variety of models used in order to try and stabilise the price of their particular stablecoin. Models include one or a combination of one of the following:

a. *Fiat token*: the issuer holds fiat currency\(^\text{42}\) equal to a portion of the total sum of tokens in issuance.

b. *Diversification/Basket*: Purchasing or tracking the price of a basket of assets including Crypto Assets, commodities, fiat currency, shares, debentures, derivatives and real estate\(^\text{43}\).

c. *Algorithm*: the issuance of the quantity of tokens (inflation) is controlled by a proprietary algorithm in consideration of various market and risk factors. These issuers attempt to mimic a central bank’s monetary policy. Others incorporate additional layers of game-theoretic incentives to encourage self-interested user behavior that would be instrumental in sustaining a ‘peg’.

---

\(^{42}\) Refer to footnote 2.

\(^{43}\) A basket of assets of such nature may meet the FSRA definition of ‘Structured Product’.
160) The rights of purchasers/issuers of stablecoins vary significantly. Some issuers retain rights to freeze client accounts for any reason, rehypothecate monies/assets at will, and provide no right of guarantee in relation to the returning of monies to clients.

**FSRA position in relation to stablecoins**

161) The FSRA position in relation to stablecoins is as follows:

a. Permit only those stablecoins which constitute a fully backed 1:1 fiat token (as referred to in paragraph 159(a) above), backed only by the same fiat currency it purports to be tokenising;

b. Fiat tokens are to be treated as a mechanism for storing value (e.g., e-money);

c. Issuers of fiat tokens for the purposes of facilitating or effecting payments are treated as money services businesses.\(^44\) In addition, to the need to hold a FSP for the Regulated Activity of Providing Money Services (see paragraph 162(a) below), the issuer will additionally be subject to relevant parts of this Guidance, including only allowing stablecoins where they meet the same requirements as those of Accepted Crypto Assets (particularly including the seven factors used to validate a Crypto Asset as an Accepted Crypto Asset as set out in paragraph 25), and that they meet wider applicable requirements as set out in this Guidance (including Technology Governance (see paragraphs 45 – 89, as applicable);

d. Require OCAB Holders to consider the wider requirements within this Guidance, and how these requirements may specially apply to the use of stablecoins, including for example, what particular risk disclosures may be relevant (see paragraphs 90-94); and

e. Continue to apply the Client Money rules in COBS to holders of Client Money (tokenised or not).

**Application of FSRA position on stablecoins to activities within ADGM**

162) A number of possible scenarios for the use of stablecoins within ADGM, and the proposed regulatory approach for each, are set out below:

a. **Issuer of fiat tokens**\(^45\): for use in the Crypto Asset ecosystem and/or as a means of payment, an Issuer (where it is located in ADGM):

i. Must seek an FSP for Providing Money Services pursuant to Schedule 1, Section 52 of FSMR;

---

\(^44\) Captured under the ‘Money Transmission’ definition (b) pursuant to Section 258 of the FSMR - selling or issuing stored value.

\(^45\) Regardless of legal personality of issuer.
ii. Is not required to become an OCAB Holder, but is required to comply with certain aspects of the OCAB Framework, namely the:

1. COB Client Money rules, and must additionally be able to show that the fiat token is backed 1:1 through weekly reconciliation; and

2. The Crypto Asset Custodian sections of this Guidance, including that the fiat token must meet the requirements applicable to Accepted Crypto Assets, Technology Governance, reconciliation and reporting (for the latter, refer to paragraph 149), and

iii. If the Issuer wishes to conduct any other OCAB activities within ADGM in addition to the issuance of a fiat token, it will need to obtain approval to become an OCAB Holder.

b. **Crypto Custodian**: that wants to hold custody over both Accepted Crypto Assets and fiat tokens:

i. OCAB Holder must operate as a Crypto Asset Custodian. No additional FSP is required to allow for the custody of fiat tokens (including for the underlying fiat currency itself). The FSRA therefore relies on the OCAB Holder meeting the:

1. OCAB capital requirements (see paragraphs 31-36);
2. OCAB Client Money rules (see paragraphs 138 - 141); and
3. requirements of this Guidance in the context of both its Accepted Crypto Asset and fiat token activities, particularly in the context of ensuring that the methods by which the OCAB Holder meets the requirements applicable to Accepted Crypto Assets and Technology Governance, and

ii. No issuance of a fiat token is permitted.

c. **Custodian providing custody/escrow services solely of a fiat currency and the related fiat token (“Fiat Custodian”):**

i. Must obtain a conventional Providing Custody FSP.

ii. Is not required to become an OCAB Holder, but is required to comply with certain aspects of the OCAB Framework, namely:

1. Being able to demonstrate that the fiat token is backed 1:1 through more frequent (weekly) reconciliations; and that

---

46 COBS Rule 17.8.3
2. Being able to demonstrate that the Accepted Crypto Asset and Technology Governance requirements are met in relation to the related fiat token.

iii. In relation to the issuance of the related fiat token, in circumstances where the issuer is not authorised under paragraph 162(a) above, it is expected that the Fiat Custodian undertake the same due diligence as that would normally apply for OCAB Holder to determine the Accepted Crypto Assets it proposes to use (focusing on Technology Governance requirements, the seven factors used to determine an Accepted Crypto Asset, and requirements relating to reporting and reconciliation).

d. **Crypto Asset Exchange: using its own fiat tokens as a payment/transaction mechanism solely within its own platform/ecosystem:**

   i. No additional FSP is required to allow for use of fiat tokens within the Crypto Asset Exchange’s platform.
   
   ii. The fiat token cannot be transferred/transacted outside its own platform/ecosystem.
   
   iii. OCAB Holder must meet the requirements of this Guidance in the context of both its Accepted Crypto Asset and fiat token activities, particularly in the context of ensuring that the methods by which the OCAB Holder meets the requirements applicable to Accepted Crypto Assets and Technology Governance, and
   
   iv. OCAB Holder must additionally be able to show that the token is backed 1:1 through weekly reconciliation.

e. **Crypto Asset Exchange: using third-party issued fiat tokens as a payment/transaction mechanism:**

   i. In the context of using third party fiat tokens, the OCAB Holder must directly meet the requirements of the Accepted Crypto Assets, Technology Governance and AML/CFT sections of this Guidance.
   
   ii. For the related fiat currency custody activities, FSRA preference is to have the Crypto Asset Exchange utilise a Crypto Asset/Fiat Custodian authorised on the basis of paragraphs 135 - 141 or 162(b) above.
   
   iii. In relation to the issuance of the related fiat token, in circumstances where the issuer is not authorised under paragraph 162(a) above, it is expected that the OCAB Holder undertake the same due diligence as that it would apply for the purposes of determining Accepted Crypto Assets (focusing on Technology Governance requirements, the seven factors used to determine an Accepted Crypto Asset, and requirements relating to reporting and reconciliation).
APPLICATION PROCESS

163) Applicants seeking to become an OCAB Holder must be prepared to engage heavily with the FSRA throughout the application process. The Application process is broadly broken down into five stages, as follows:
   a) Due Diligence & Discussions with FSRA team(s);
   b) Submission of Formal Application;
   c) Granting of In Principle Approval;
   d) Granting of Final Approval; and
   e) ‘Operational Launch’ Testing

Due diligence and Discussions with FSRA team(s)

164) Prior to the submission of an Application, all Applicants are expected to provide the FSRA with a clear explanation of their proposed business model and to demonstrate how the Applicant will meet all applicable FSRA Rules and requirements. These sessions will also involve the Applicants providing a number of in-depth technology demonstrations, across all aspects of its proposed OCAB activities. The FSRA generally expects these meetings, where possible, to take place between the Applicant and the FSRA in person. Given the complexity of the activities associated with the OCAB Framework, it is likely that a number of meetings will need to be held between an Applicant and the FSRA before the Applicant will be in a position to submit a draft, then formal, application.

Submission of Formal Application

165) Following discussions with the FSRA, and upon the FSRA having reasonable comfort that the Applicant’s proposed business processes, technologies and capabilities are at a sufficiently advanced stage, the Applicant will be required to submit a completed OCAB Application Form, and supporting documents, to the FSRA. Payment of the fees applicable to the Application, as set out in paragraphs 171 - 179, must also be made at the time of submission. The FSRA will only consider an Application as having been formally submitted, and commence its formal review of the Application, upon receipt of both the completed Application and the associated fees.

Granting of In Principle Approval (IPA)

166) The FSRA will undertake an in depth review of the Application, and supporting documents, submitted by an Applicant. The FSRA will only consider granting an IPA for a FSP for OCAB for those Applicants that are considered able to adequately meet all applicable Rules and requirements. An Applicant will be required to meet all conditions applicable to the IPA prior to being granted with final approval and an FSP for OCAB.

47 The FSRA will make available to the Applicant an editable version of the OCAB Application Form at the appropriate time. Other ancillary forms to be submitted include the Approved Person Status form (for appointing Controlled Functions such as the SEO and Licensed Directors) and the Recognized Person Status form (for appointing Recognised Functions such as the Compliance Officer, MLRO and Finance Officer).
Granting of Final Approval (Financial Services Permission)

167) Subject to being satisfied that the Applicant has met all conditions applicable to the IPA, the FSRA will grant the Applicant with final approval for an FSP for OCAB. Final approval will be conditional upon the FSRA being further satisfied in relation to the Applicant’s operational testing and capabilities, and completion of a third party verification of the Applicant’s systems where applicable.

‘Operational Launch’ Testing

168) An Applicant (particularly a Crypto Asset Exchange and/or Crypto Asset Custodian) will only be permitted to progress to operational launch when it has completed its operational launch testing to the FSRA’s satisfaction, including completion of third party verification of the Applicant’s systems, where applicable.

169) Noting the heightened risks associated with activities related to OCAB, OCAB Holders will be closely supervised by the FSRA once licensed. OCAB Holders will be expected to meet frequently with the FSRA, will be subject to ongoing assessments and should be prepared to undergo thematic reviews from time to time.

Opening a bank account

170) Given the associated risks within the Crypto Asset space, the global banking sector is focusing on account opening requests from entities associated with Crypto Assets with increased scrutiny. The FSRA has engaged in extensive discussions with local and international banks for the purposes of providing an overview of the OCAB Framework and the stringent authorisation requirements imposed on Applicants when applying to become an OCAB Holder. It is intended that those banks with a risk appetite to bank Crypto Asset players will glean comfort from the regulatory oversight of the FSRA and the issuance of an IPA to entities demonstrating that they have a clear roadmap of development of their business towards final approval and issuance of an FSP. The process for approval for the opening of a bank account with local or international banks will typically include a full explanation and review of an Applicant’s AML and Client on-boarding processes and procedures, as well as its ability to monitor the source and destination of funds, amongst other areas of its OCAB activities.

FEES

Authorisation and supervision fees

171) The Fees applicable to OCAB Holders have been established in consideration of the risks involved in relation to Crypto Asset activities and the supervisory requirements placed on the FSRA to suitably regulate OCAB Holders and Crypto Asset activities in ADGM.
Pursuant to FEES Rule 3.14.1, an Applicant for an FSP to carry on the Regulated Activity of Operating a Crypto Asset Business must pay, at the time of submission of its Application, an initial authorisation fee of (as applicable):

f) $20,000; or

g) $125,000 if the Applicant is seeking to operate as a Crypto Asset Exchange.

As set out earlier in paragraph 165, the FSRA will only consider an Application as having been formally submitted, and commence its formal review of the Application, upon receipt of both the completed Application and the associated fees.

Pursuant to FEES Rule 3.14.2, annual supervision fees, payable in accordance with paragraph 1 of the FEES Rulebook, are set as follows:

a) $15,000; or

b) $60,000 if the Applicant is seeking to operate as a Crypto Asset Exchange.

Cumulative application of Fees

Subject to paragraph 177 below, if an Applicant/OCAB Holder will be undertaking multiple OCAB activities as part of its FSP, the fees (authorisation and supervision) payable by that OCAB Holder will be cumulative, and considered across the following:

a) intermediary activities set out in sub-paragraphs (a) – (e) of section 73B of Schedule 1 of FSMR (as outlined in paragraph 15 of this Guidance) (being “Non-Custody OCAB Intermediary Activities”);

b) activities as a Crypto Asset Custodian; and

c) activities as a Crypto Asset Exchange.

In practice, and to further clarify, this results in several scenarios relating to fees, being:

a) Non-Custody OCAB Intermediary Activities only = Application Fee of $20,000 and annual supervision fee of $15,000 (irrespective of the number of Non-Custody OCAB Intermediary Activities proposed to be undertaken).

b) Crypto Asset Custodian and Non-Custody OCAB Intermediary Activities = Application fee of $40,000 and annual supervision fee of $30,000.

c) Crypto Asset Exchange = Application fee of $125,000 and annual supervision fee of $60,000.

d) Crypto Asset Exchange and Crypto Asset Custodian = Application fee of $145,000 and annual supervision fee of $75,000.
177) Noting the above paragraph, if an Applicant/OCAB Holder will be undertaking conventional Regulated Activities in addition to its OCAB activities, as noted in paragraphs 20 to 21, a license will therefore be required to include both conventional Regulated Activities as well as OCAB activities. The fees attributable to that OCAB Holder for its Regulated Activities, conventional and OCAB, will be cumulative.

178) Pursuant to FEES Rule 3.14.3, a Crypto Asset Exchange must pay to the FSRA a trading levy on a sliding scale basis (as set out in the table below), payable monthly in USD. Unless otherwise determined by a Crypto Asset Exchange, the FSRA expects that the calculation of average daily value should occur at 12am Abu Dhabi time (+4hr GMT).

<table>
<thead>
<tr>
<th>Average Daily Value (ADV) ($USD)</th>
<th>Levy</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADV ≤ 10m</td>
<td>0.0015%</td>
</tr>
<tr>
<td>10m &lt; ADV ≤ 50m</td>
<td>0.0012%</td>
</tr>
<tr>
<td>50m &lt; ADV ≤ 250m</td>
<td>0.0009%</td>
</tr>
<tr>
<td>ADV &gt; 250m</td>
<td>0.0006%</td>
</tr>
</tbody>
</table>

179) Pursuant to FEES Rule 1.2.6(a), the FSRA reserves its right to impose additional fees in circumstances where a ‘substantial additional’ regulatory burden is imposed on FSRA. In such circumstances, including the migration of a Crypto Asset Exchange to become a conventional ‘Securities’ Recognised Investment Exchange, the FSRA recommends that the Applicant/OCAB Holder discuss FEE implications with the FSRA as early as practicable.