FINANCIAL SERVICES REGULATORY AUTHORITY
سلطة تنظيم الخدمات المالية

Guidance – Regulation of Crypto Asset Activities in ADGM

DATE: 25 June 2018

Table of Contents

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'*[1] ("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; or

   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.

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, as applicable, intermediaries engaged in Crypto Asset activities. This Guidance, together with the applicable ADGM Regulations and FSRA Rules governing Crypto Asset activities, is collectively referred to as the "Spot Crypto Asset 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; or

   b) waive or modify any of these requirements 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").

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 93) are each referred to as an "OCAB Holder".

[1] https://www.adgm.com/media/304700/guidance-icos-and-crypto-assets_20180625_v11.pdf

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 digital assets, such as virtual coins or tokens for capital raising, and crypto assets/currencies for the facilitation of economic transactions.

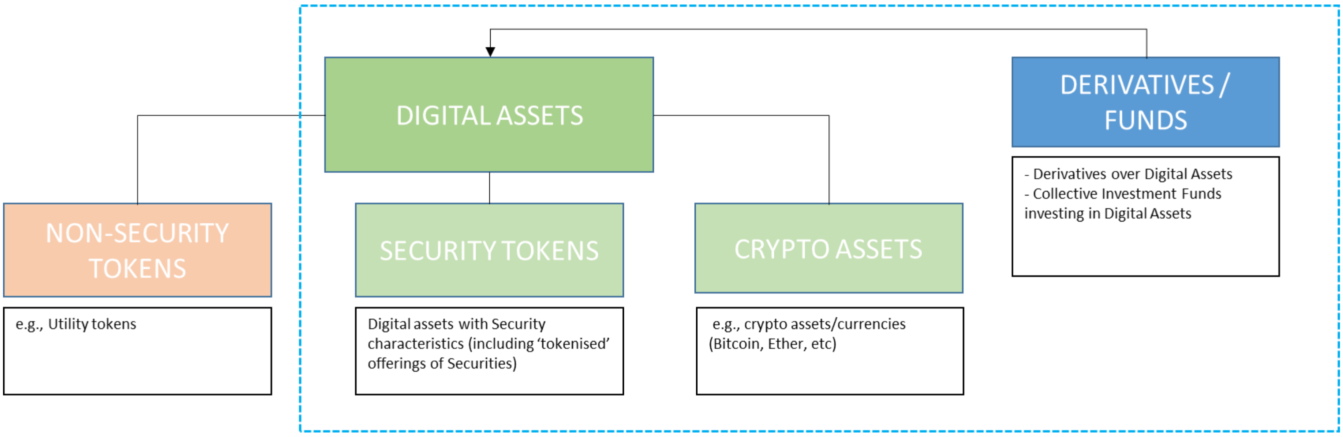
9) This Guidance focuses on FSRA's regulatory treatment of Crypto Assets. For the purposes of the Spot Crypto Asset Framework, the FSRA has defined Crypto Asset in the FSMR as follows:

*"**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 Currency[2] and E-money[3]."

10) The diagram and table below sets out the FSRA's regulatory approach in relation to different types of digital assets.


DIGITAL ASSETS
DERIVATIVES / FUNDS
- Derivatives over Digital Assets
- Collective Investment Funds investing in Digital Assets
NON-SECURITY TOKENS
e.g., Utility tokens
SECURITY TOKENS
Digital assets with Security characteristics (including 'tokenised' offerings of Securities)
CRYPTO ASSETS
e.g., crypto assets/currencies (Bitcoin, Ether, etc)

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

[3] "E-money" means a digital representation of Fiat Currency used to electronically transfer value denominated in Fiat Currency. The FSRA considers E-money activities to be covered by its payments regulatory framework.

Category of Digital Assets / Instruments	**Regulatory Approach**
"Security Tokens" (e.g., virtual tokens that have the features and characteristics of a Security under the FSMR (such as Shares, Debentures, Units in a Collective Investment Fund)).	Deemed to be Securities pursuant to Paragraph 58(2)(b) of FSMR. All financial services activities in relation to Security Tokens, such as operating primary / secondary markets, dealing / trading / managing investments in or advising on Security Tokens, will be subject to the relevant regulatory requirements under the FSMR. Market intermediaries and market operators dealing or managing investments in Security Tokens need to be licensed / approved by FSRA as FSP holders, Recognised Investment Exchanges or Recognised Clearing Houses, as applicable.
"Crypto Assets" (e.g., non-fiat virtual currencies). *As provided in paragraph 9, this Guidance is focused on Crypto Assets.*	Treated as commodities and, therefore, not deemed Specified Investments under the FSMR. Pursuant to the Spot Crypto Asset Framework, however, market intermediaries (e.g. broker dealers, custodians, asset managers) and Crypto Asset Exchanges dealing in or managing Crypto Assets will need to be licensed / approved by FSRA as OCAB Holders. Only activities in Accepted Crypto Assets will be permitted.
"Utility Tokens" or "Non-Security Tokens" (e.g., virtual tokens that 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 under the definition of 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 the Market Rules (MKT).
Derivatives and Collective Investment Funds of Crypto Assets, Security Tokens and Utility Tokens	Regulated as Specified Investments under the FSMR. 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.

11) For clarification, the Spot Crypto Asset Framework is not intended to apply to initial token or coin offerings (ICOs), (whether Security or Utility tokens), or other capital raising

purposes. For details on FSRA's regulatory treatment of ICOs, security tokens and utility tokens please refer to FSRA's ICO Guidance.

OBJECTIVES OF THE SPOT CRYPTO ASSET 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 enables 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 Spot Crypto Asset Framework is comprehensive in order to effectively address the key risks that spot 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 of 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 currently no 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 exchanges globally.

FEATURES OF THE SPOT CRYPTO ASSET FRAMEWORK

Regulated Activity of Operating a Crypto Asset Business

15) In accordance with section 30 of FSMR, Applicants that qualify for authorisation under the Spot Crypto Asset 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 and 73C 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;

(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.'

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 considered by the FSRA to be 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, Rule 17.1.2 operates as an additional '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 Spot Crypto Asset Framework.

RISK		MITIGANT
1.	**AML/CFT/TAX**	The AML Rulebook applies in full to the Regulated Activity of OCAB. OCAB Holders will also need to consider their reporting obligations in relation to FATCA and the Common Reporting Standards.
2.	**CONSUMER PROTECTION**	All material risks associated with Crypto Assets generally, Accepted Crypto Assets and OCAB products, services and activities must be appropriately disclosed.
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 will be regulated in a similar manner to how the FSRA regulates 'Multilateral Trading Facilities', and will be required to have in place, among other things, the following: • Market surveillance; • Settlement processes; • Transaction recording; • Transparency & public disclosure mechanisms; and • Exchange-like operational systems and controls.
5.	**CUSTODY**	Crypto Assets will be included as Client Assets and Investments, and accordingly will be subject to the safe custody provisions under the FSMR. Frequent reconciliations and reporting of Crypto Assets 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 to be 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 carrying on other Regulated Activities within ADGM in addition to OCAB will need to apply to add such other Regulated Activities to the FSP and comply with the requirements of the FSRA applicable to such other Regulated Activities.

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

REGULATORY REQUIREMENTS FOR OPERATING A CRYPTO ASSET BUSINESS

Operating a Crypto Asset Business

22) Chapter 17 of COBS applies to all OCAB Holders, requiring compliance with all the 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 in COBS Rule 17.7 or 17.8 respectively.

Accepted Crypto Assets

23) 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 higher-risk activities involving or relating to illiquid or 'immature' Crypto Assets.

24) A Crypto Asset that meets the FSRA's requirements will constitute an Accepted Crypto Asset. 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:

   a) A maturity/market capitalisation threshold in respect of a Crypto Asset in accordance with COBS Rule 17.2.2(a). This market capitalisation threshold will be applied at the time of application for an FSP to engage in the Regulated Activity of OCAB. The FSRA considers Crypto Assets with a market capitalisation in excess of at least US$4billion[4] as meeting this threshold. 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.

b) Other factors that, in the opinion of the FSRA, need to be taken into account in determining whether or not a particular Crypto Asset meets the requirements to be considered appropriate, as contemplated in COBS Rule 17.2.2(b). The FSRA will take into account a number of factors in relation to a particular Crypto Asset, including those set out below, none of which are to be considered definitive or binding:

i. Security: consideration of whether the 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);

ii. 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 trade, and if transactions in the Crypto Asset can be adequately monitored;

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

iv. Market demand / volatility: 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;

v. Type of Distributed Ledger: whether there are issues relating to the security and/or usability of a distributed ledger technology used for the purposes of the Crypto Asset; whether the Crypto Asset leverages an existing distributed ledger for network and other synergies; whether this a new distributed ledger that has been demonstrably stress tested;

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

vii. Practical application/functionality: whether the Crypto Asset possesses real world, quantifiable, functionality.

25) 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.

[4] www.coinmarketcap.com

26) 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. The use of these Accepted Crypto Assets will be approved as part of the formal application process for its FSP for Operating a Crypto Asset Business.

27) An Accepted Crypto Asset may be deemed suitable for use by all OCAB Holders, subject to each OCAB Holder satisfying the FSRA that it can suitably use each specific Accepted Crypto Asset. For example, a Crypto Asset Exchange is required by COBS Rule 17.7.4[5] 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.

28) 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 notify the FSRA of its intention to do so. This notification should 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 the 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 of being an Accepted Crypto Asset, as set out in COBS Rule 17.2.2 and paragraph 24 of this Guidance. The FSRA will notify the OCAB Holder of its determination.

29) The FSRA will not maintain a 'public' list of Accepted Crypto Assets, however it may provide this information to potential Applicants of an OCAB FSP, and OCAB Holders.

Capital Requirements

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

31) 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 capital required as the additional buffer. An OCAB Holder that the FSRA considers to be high risk may attract higher capital requirements.

32) Subject to the above paragraph, in general:

[5] Which requires notification to the FSRA under MIR Rule 5.4.1 (Item 26).

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

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

33) Operational expenses, as set out in MIR Rule 3.2.1, broadly includes 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 accounting 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.

34) Where an OCAB Holder carries on one or more Regulated Activities not related to Crypto Asset activities (e.g., Dealing in Investments, Providing Credit or Providing Custody etc.), the FSRA will apply a capital requirement that is the higher of the:

a) regulatory capital requirements applicable to the OCAB; or

b) capital requirements applicable to the other Regulated Activities under the "Prudential – Investment, Insurance Intermediation and Banking Rules" ("PRU").

35) 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 for the Group pursuant to Chapter 8 of PRU. The resulting level of the capital requirements 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

36) Crypto Asset activities raise significant regulatory concerns for regulatory authorities and law enforcement agencies worldwide, particularly in relation to Money Laundering ("ML") and Financing of Terrorism ("TF"). International bodies, such as the International Monetary Fund, the Financial Action Task Force ("FATF"), the Bank for International Settlements 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 illegal purposes.

37) FATF has identified certain key risks associated with Crypto Assets[6], which include the following:

[6] http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

a) Digital Assets (and, in particular, Crypto Assets) usually provide greater anonymity than traditional non-cash payment methods. Crypto Assets can be traded via Internet platforms, are generally characterised by non-face-to-face Client relationships, and may permit anonymous funding and transfers (cash funding or third-party funding through 'virtual exchanges' that do 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 spread across several 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, often 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.

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

38) 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. (38) of 2014 Concerning the Executive Regulation of the Federal Law No. 4 of 2002 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).

39) In considering 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.

Key considerations for AML/CFT compliance

40) 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 OCAB Holders establish proper systems and controls, 'Know-Your-Client' ("KYC") and 'Client Due Diligence' ("CDD") processes, and build their policies and procedures to be risk focused and proportionate to their activities.

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 a financial institution is how the on-boarding of an OCAB Holder may affect its relationship with a foreign correspondent financial institution, as well as the views of the regulator of that foreign correspondent financial institution. 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, a financial institution of an OCAB Holder must not only satisfy itself, but also its foreign correspondent financial institutions, that OCAB Holders are well regulated and have systems and controls to address ML, TF and sanctions risks. This should include robust processes to carry out CDD on customers and beneficial owners, monitor transactions for these risks, and be willing and able to provide complete transparency to their financial institution and its foreign correspondent financial institutions 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 money laundering 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[7] 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 'technical' 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, consumer protection, etc).

Principle 3: Know Your Customer, Customer Due Diligence and Customer Risk Assessment

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 anonymity features, which makes tracking Client records and transactions more challenging for compliance officers and money laundering reporting officers.

i) Clear KYC and CDD policies and procedures are required to be implemented. OCAB Holders should have a process to assess and rate their Clients according to that Client's risk profile (and taking into consideration the OCAB Holder's RBA). This process requires OCAB Holders to undertake CDD and comply in full with AML Rules 8.1 and 8.3 for each Client prior to transacting any business whatsoever. The FSRA does not consider it appropriate for OCAB Holders to use simplified CDD when conducting Crypto Asset activities.

j) Due to issues surrounding the anonymity of Clients and transactions associated with Crypto Assets, when considering CDD and the treatment of third party funding of Client accounts, the FSRA draws OCAB Holders' particular attention to AML Rule

[7] Examples of Digital Asset/Crypto Asset relevant terminology include: cold or hot storage, on/off ramps, dirty wallet, public key and private key.

8.1.3 (Guidance paragraph 3)[8] noting that the FSRA will apply the Rule such that there is no exception for simplified CDD.

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. The use of suitable biometric technologies for non-face-to-face business activity may be acceptable to the FSRA in certain cases.

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 KYC and CDD requirements are not appropriately undertaken by an OCAB Holder.

Principle 4: Governance, Systems and Controls

m) OCAB Holders are required to implement an appropriate governance structure, especially in relation to Information Technology governance[9], and provide for the development and maintenance of all necessary systems and controls to ensure appropriate ML and TF compliance.

n) The FSRA expects that OCAB Holders may seek to utilise technologies and solutions available in the market to meet their regulatory obligations (e.g., KYC, detection of fraud, transaction identification and reporting) and risk management requirements (e.g., margin limits, large exposure monitoring).

o) While 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 will be generated within the Crypto Asset industry itself.

[8] AML Rule 8.1.3 Guidance 3 states that '*Subject to the exception for Simplified Customer Due Diligence, whenever a Relevant Person comes into contact with a Customer with or for whom it acts or proposes to act,* ***it must establish whether the Customer is acting on his own behalf or on behalf of another Person, and a Relevant Person must establish and verify the identity of both the Customer and any other Person on whose behalf the Customer is acting, <u>including that of the Beneficial Owner of the relevant funds</u>, which may be the subject of a Transaction to be considered, and must obtain sufficient and satisfactory evidence of their identities****. A Relevant Person should obtain a statement from a prospective Customer to the effect that he is, or is not, acting on his own behalf. In cases where the Customer is acting on behalf of third parties, it is recommended that the Relevant Person obtain a written statement, confirming the statement made by the Customer, from the parties, including the Beneficial Owner.'*

[9] Please also refer to the section on Technology Governance and Controls in this Guidance (page 18).

p) 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 and as robust as possible. The policy can be separate or part of other compliance policies/manuals.

q) 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.

r) 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: Reporting obligations

s) OCAB Holders should familiarise themselves with their reporting obligations under the AML Rules, in particular in relation to the reporting of suspicious activities/transactions.

t) 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

u) 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.

v) The FSRA understands that the transaction recording of many Crypto Asset transactions is linked to, or based on, blockchain technology. 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 blockchain to store its data, provided it is able to provide this data, in an easily accessible format, to the FSRA when required.

w) 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, or prohibitions on the receipt of cash other than from bank accounts. 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.

x) 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 regulatory risk or reputational damage to the ADGM Financial System.

International Tax Reporting Obligations

41) 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

42) While the FSRA adopts a technology-neutral approach to its regulation of Authorised Persons, 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.

43) Historic Crypto Asset business failures have often arisen as a result of the lack of adequate technology-related procedures, including for example, a lack of code version control, lack of testing or security policies, or a lack of an appropriate framework for decision making. The FSRA has therefore included specific Guidance regarding expected controls and processes to mitigate these issues.

44) 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 regular 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.

45) 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, 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

46) OCAB Holders are expected to have a clear, well-structured and deliberate approach for the implementation and upgrade of systems and software.

47) 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”) with a third party). This should include ensuring that the implementation of new systems, or upgrading of existing systems, is thoroughly checked by multiple members of technology staff.

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

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

50) OCAB Holders should conduct at least annual third-party audit of core systems being used. 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

51) OCAB Holders should have measures and procedures in place which comply with network security best practices (e.g., the implementation of firewalls, the regular changing of passwords and encryption of data in transit and at rest). 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.

52) 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. IT infrastructures should be strong enough to resist, without significant loss to customers, a number of scenarios, including but not limited to: accidental destruction or breach of a single facility, collusion or leakage of information by employees/former employees within a single office premise, successful hack of a cryptographic module or server, or access by hackers of any single set of encryption/decryption keys.

53) OCAB Holders should regularly test security systems and processes. Vulnerabilities are being introduced continually by malicious individuals and researchers, often via new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

54) OCAB Holders should have in place policies and procedures that address information security for all personnel. A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

55) The encryption of data, both at rest and in transit, including consideration of API security (e.g. OAuth 2.0) should be included in the security policy. In particular, encryption and decryption of Crypto Asset private keys should utilise encryption protocols, or use alternative 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 ideally internationally recognised, applicable security standards.

56) OCAB Holders should conduct regular (at least annually) security tests of their systems, network, and connections.

Cryptographic Keys and wallet storage

57) Distributed ledgers, which are considered to be the single source of truth regarding ownership of Crypto Assets, are often based on blockchain technology. 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 generation, storage, backup and destruction of both public and private keys.

58) To be able to access Crypto Assets, the device on which the private key is held needs access to a network (which, in most cases, will be via the internet). A wallet where the private key is held on a network attached device is called a hot wallet. Hot wallets are vulnerable to hacking attempts and can be more easily compromised by viruses and malware. Crypto Assets that do not need to be immediately available should be held off line, in a 'cold wallet' to the extent feasible. Below is a non-exhaustive list of some of the measures that OCAB Holders should consider:

Password protection and encryption

59) Both hot and cold wallets must be password protected and encrypted. The key storage file that is held on the online or offline device is generally encrypted. The user is therefore protected against theft of the file (to the degree the password cannot be cracked), but malware on the machine may still be able to gain access (e.g., a keystroke logger to capture the password).

60) 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). Noting that there is no way to recover stolen or lost private keys unless a copy of that key has been made, multi-signature wallets may offer more security because a user can still gain access to its Crypto Assets when two or more Private Keys remain available.

Off line storage of keys

61) To mitigate the risks associated with hot wallets, private keys can be stored in a cold wallet, which is not attached to a network. OCAB Holders should implement cold wallet key storage where possible if they are offering wallet services to their Clients.

Air gapped key storage

62) Wallets may also be stored on a secondary device that is never connected to a network. This device, referred to as an air-gapped device, is used to generate, sign, and export transactions. Care must be taken not to infect the air-gapped device with malware when, for example, inserting portable media to export the signed transactions. Hardware security modules emulate the properties of an air gap. A proper policy must be created to describe the responsibilities, methods, circumstances and time periods within which transactions can be initiated. Access and control of single private keys should be shared by multiple users to avoid transactions by a single user.

Password-derived keys

63) Some wallet solutions enable cryptographic keys to be derived from a user-chosen password (the "seed") in a "deterministic" wallet. The most basic version requires one password per key pair. A Hierarchical Deterministic wallet derives a set of keys from a given seed. The seed allows a user to restore a wallet without other inputs. An OCAB Holder offering deterministic wallet solutions should ensure that users are provided with clear instructions for situations where keys, seeds or hardware supporting such wallet solutions are lost.

Origin and destination of Crypto Asset funds

64) Crypto Asset transactions between public addresses take place on a public distributed ledger. 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 financers and other criminals.

65) 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.[10] Additionally, there are companies collecting "tainted" wallet addresses that have been used in hacks, "dark web" transactions and other criminal endeavours.

66) 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).

67) 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 consider the use of third party services to help identify such addresses.

68) 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. OCAB Holders should consider using such solutions and other systems to adequately meet anti-money laundering, financial crime and know-your-customer requirements set out in the Spot Crypto Asset Framework.[11]

[10] https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx

[11] For full details on these obligation, please refer to the earlier section of AML/CFT.

Planned and Unplanned system outages

69) 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.

70) 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.

Management of personnel and decision making

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

72) 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.

73) 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

74) 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.

75) 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).

76) 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.

Crypto Asset Risk Disclosures

77) 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.

78) COBS Rule 17.6 sets out a non-exhaustive list of risks that are required to be disclosed to Clients. 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[12];

b) Crypto Assets generally; and

c) the specific Accepted Crypto Asset.

79) 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).

80) 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.

Market Abuse, Transaction Reporting and Misleading Impressions (FSMR)

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

82) 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

[12] 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 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.

to Crypto Assets traded on Crypto Asset Exchanges as it does to Financial Instruments traded on Recognised Investment Exchanges, MTFs or OTFs in ADGM.

83) An important change to assist the FSRA with the prevention, monitoring and enforcement of these Market Abuse provisions is set out in FSMR Section 149. Similar to the reporting requirements imposed on Recognised Investment Exchanges and MTFs, Crypto Asset Exchanges are also required to report details of transactions in Accepted Crypto Assets traded on their platforms.[13] The FSRA will expect Crypto Asset Exchanges to report on both a real-time and batch basis.

84) 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 will be made in an appropriate manner and that an Authorised Person will implement suitable policies and procedures to comply with the requirements of FSMR.

Application of particular Rules in COBS

85) For the purposes of the Spot Crypto Asset 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);

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)).

86) These requirements are relevant to the concept of 'Investment Business' within COBS, and are to be applied to the activities of all OCAB Holders. The FSRA appreciates that some of these individual obligations may not apply to certain OCAB Holders and will, where necessary and appropriate, consider granting modification or waiver relief to OCAB Holders.

CRYPTO ASSET EXCHANGES

87) 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

[13] The additional obligation of a Crypto Asset Exchange to undertake its own market surveillance is set out later in paragraph 90(d) of this Guidance.

activity in ADGM. For this reason, the Spot Crypto Asset 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").

88) The FSRA considers that operating a Crypto Asset Exchange within ADGM cannot be undertaken by entities without a commitment of substantial resources, including a substantial commercial, governance, compliance, technical, IT and HR presence, within ADGM.

89) 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[14].

90) Chapter 8 of COBS incorporates Rules from various other FSRA Rulebooks that must be complied with, including certain sections of the Market Infrastructure Rules ("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 42 to 76 of this Guidance, such that the FSRA's expectations in this area are similar to what is expected of Recognised Investment Exchanges 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 extensive due diligence and testing of a Crypto Asset Exchange's operational systems to be undertaken, 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 the appropriate expertise. 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

[14] 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.

Asset Exchange's systems with other parties. Testing 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 and an internal ledger maintained by a Crypto Asset Exchange, 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'*.

i. MIR Rules 2.8.2 to 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 Members (e.g., access is granted directly to Clients of the Crypto Asset Exchanges). A Crypto Asset Exchange will, therefore, need to ensure that it has appropriate processes, controls and Rules to 'protect the orderly functioning' of the 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 have, in that they do not have Members assisting them by undertaking the necessary due diligence and compliance reviews of investors in 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 (something which a Recognised Investment Exchange may rely on its Members to do). Resultant AML/CFT obligations therefore also fall more directly on a Crypto Asset Exchange as well. The FSRA expects that the controls (and resultant resourcing needs) be appropriately accounted for by Crypto Asset Exchanges.

iv. Depending on the model, controls and criteria to be adopted by a Crypto Asset Exchange, the FSRA may be minded to consider granting modification or waiver relief in relation to the specific 'Member' requirements in MIR Rule 2.8.

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 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 associated resourcing needs required to undertake these functions appropriately.

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.[15]

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 any 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): Any arrangements of a Crypto Asset Exchange used to make information public (including trading information required to be disclosed under COBS 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.

[15] Refer to paragraphs 81 to 84 of this Guidance.

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 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.

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 Member/Client is unable to meet its obligations in respect of transactions relating to Accepted Crypto Assets.

91) 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 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 28 of this Guidance in relation to the use of additional Accepted Crypto Assets.

92) It is recognised that Crypto Asset Exchanges may take varying approaches in relation to the custody of fiat currencies and Crypto Assets. In some circumstances, a Crypto Asset Exchange may use third party custodians. However, to the extent that a Crypto Asset Exchange conducts its own custody activities, it 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 section below on "Crypto Asset Custodians".

Recognised Investment Exchanges Operating a Crypto Asset Exchange

93) 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 Spot Crypto Asset 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.

94) This means that a Recognised Investment Exchange can, where permitted by the FSRA and subject to MIR Rule 3.4.2, operate an MTF, OTF and/or Crypto Asset Exchange under its Recognition Order.

CRYPTO ASSET CUSTODIANS

95) 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 Spot Crypto Asset Framework contains specific additional requirements applicable to Crypto Asset Custodians.

96) 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 Crypto Assets are afforded the same protections as other similar products and activities under FSMR and the FSRA Rulebook.

97) The FSRA notes that there are broadly three types of custodial arrangements (for Crypto Assets) that OCAB Holders are likely to adopt:

a) Type 1: The OCAB Holder is wholly responsible for custody of Client’s 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 Crypto Assets bought through that exchange or transferred into the wallet from other sources.

b) Type 2: The OCAB Holder is wholly responsible for the custody of Client’s Crypto Assets but outsources this service to a third-party Crypto Asset Custodian. Such an arrangement includes the scenario where a Crypto Asset Exchange uses a third party service provider to hold all its Clients’ Crypto Assets (e.g., all or part of the Clients’ private keys).

c) Type 3: The OCAB Holder wholly allows Clients to “self-custodise” their Crypto Assets. Such an arrangement includes scenarios where some **distributed** Crypto Asset Exchanges require Clients to self-custodise their Crypto Assets. Such exchanges only provide the trading platform for Clients to buy and sell Crypto Assets; Clients are required to source and use their own third party Crypto Asset Custodians (which the distributed Crypto Asset Exchanges have no control over or responsibility for). This arrangement also includes the scenario where OCAB Holders (such as Crypto Asset Exchanges) provide an in-house wallet service for Clients, but also allow Clients to transfer their Crypto Assets out of this wallet to another wallet from a third party wallet provider chosen by the Client (and which the OCAB Holder does not control).

98) The FSRA considers scenarios where Clients are required to self-custodise their Crypto Assets as being 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 77 to 80 in the section of this Guidance above on "Crypto Asset Risk Disclosures". The FSRA will take the quality of these disclosures into account when assessing applications from OCAB Holders proposing to require Clients to self-custodise their Crypto Assets.

Protection of Client Money

99) Chapter 14 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 Money that they are holding or controlling on behalf of their Clients. In addition, COBS Rule 17.8 describes how the Client Money rules in Chapter 14 apply to Crypto Asset Custodians.

100) "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.

101) 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 his trading account at a Crypto Asset Exchange, a Client of the Crypto Asset Exchange transfers US dollars (in fiat) from his bank account to his 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.

b) Example 2: A Client of a Crypto Asset Exchange holds bitcoins in his wallet at the Crypto Asset Exchange. He uses the Crypto Asset Exchange to sell these bitcoins in exchange for US dollars (in fiat). The US dollars are then credited to his account at the Crypto Asset Exchange and held by the Crypto Asset Exchange for him. These US dollars held in his account with the Crypto Asset Exchange would be considered Client Money.

102) 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 COBS Rule 17.8) at all times. 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

103) 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 describes how the Safe Custody rules in Chapter 15 apply to Crypto Asset Custodians.

104) "Client Investments" in the context of Crypto Asset Custodians refer specifically to Crypto Assets such as bitcoin and not to money (in fiat) of any currency. Refer to paragraphs 99 to 102 above for guidance on how Crypto Asset Custodians are required to properly protect and safeguard Client Money (in fiat).

105) The following are examples of situations where a Crypto Asset Custodian would be considered to be holding, controlling, providing custody for, or arranging custody for, with respect to Accepted Crypto Assets, on behalf of its Clients:

a) <u>Example 1</u>: A Client of a Crypto Asset Exchange uses US dollars (in fiat) to purchase bitcoins on the Crypto Asset Exchange. The Crypto Asset Exchange provides an integrated Crypto Asset wallet service to the Client, and holds the bitcoins for the Client in this wallet. The Crypto Asset Exchange may also allow the Client to transfer bitcoins from other wallets to the wallet held with the Crypto Asset Exchange, or from the Crypto Asset Exchange's wallet to these other wallets.

b) <u>Example 2</u>: A Crypto Asset wallet provider (being a Crypto Asset Custodian) that is not a Crypto Asset Exchange offers a dedicated Crypto Asset wallet service, allowing the Client to transfer bitcoins purchased on a Crypto Asset Exchange or received from another person, to the wallet. The crypto wallet provider keeps these bitcoin in custody for the Client. Crypto Asset Exchanges may also outsource such service.

106) There are currently two main types of Crypto Asset wallets:

a) <u>Type 1: "Custodial Wallets" -</u> the custodial wallet provider holds Crypto Assets (e.g., the private keys) as an agent on behalf of Clients, and has at least some control over these Crypto Assets. Most Crypto Asset Exchanges that hold Crypto Assets on behalf of their Clients would generally be offering Custodial Wallets and often offer multi-signature wallets (please see paragraph 60). Clients using custodial wallets do not necessarily have full and sole control over their Crypto Assets. In addition, there is a risk that should the custodial wallet provider cease operations or get hacked, Clients may lose their Crypto Assets.

b) <u>Type 2: "Non-Custodial (Self-Custody) Wallets"-</u> the non-custodial wallet provider, typically a third-party hardware add/or software company, offers the means for each Client to hold their Crypto Assets (and fully control private keys) themselves. The non-custodial wallet provider does not control Client's Crypto Assets – it is the Client that has sole and full control over their Crypto Assets. 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' authorization.

107) Only entities providing the custodial wallets as described in paragraph 106(a) above are considered to be carrying out the regulated activity of a Crypto Asset Custodian. With respect to the non-custodial wallets as described in paragraph 106(b) 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.

108) An OCAB Holder that holds, controls, provides custody for, or arranges custody for, with respect to 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.

109) Crypto Asset Exchanges that provide an integrated Crypto Asset wallet would also need to comply with these Safe Custody rules. Crypto Asset Exchanges that outsource their Crypto Asset wallets to a third party may also be considered as "arranging custody", and may also need to comply with these Custody Rules, as applicable.

110) In addition to the two main Crypto Asset wallet types described above, the FSRA recognises that there may be alternative Crypto Asset wallet models in existence or which may emerge in future. Entities seeking to provide such alternative types of Crypto Asset wallets and who are unsure of the regulatory obligations they may attract are encouraged to contact the FSRA.

111) OCAB Holders operating as Crypto Asset Custodians are required to:

a) Send out statements of a Client's 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 Crypto Asset holdings at least every week (as required under COBS Rule 15.9.1).

FEES

112) 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.

113) 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 an initial authorisation fee of (as applicable):

a) $20,000; or

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

114) Pursuant to FEES Rule 3.14.2, annual supervision fees are set as follows:

a) $15,000; or

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

115) If an Applicant/OCAB Holder will be undertaking multiple OCAB Regulated Activities as part of its FSP, the fees attributable to that OCAB Holder will be cumulative. This means, for example, where an Applicant is seeking to operate as a Crypto Asset Exchange and a Crypto Asset Custodian, the $20,000 authorisation fee attributable to a Crypto Asset Custodian would be added to the $125,000 authorisation fee attributable to the Crypto Asset Exchange.

116) Noting the above paragraph, if an Applicant/OCAB Holder will be undertaking conventional Regulated Activities in addition to its OCAB activities, as noted in paragraph 20 a licence will be required to include the conventional Regulated Activities as well as the OCAB activities. The fees attributable to that OCAB Holder for its Regulated Activities, conventional and OCAB, will be cumulative.

117) 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.

Average Daily Value (ADV) ($USD)	**Levy**
ADV ≤ 10m	0.0015%
10m < ADV ≤ 50m	0.0012%
50m < ADV ≤ 250m	0.0009%
ADV > 250m	0.0006%

118) In circumstances where a Recognised Investment Exchange seeks to also operate a Crypto Asset Exchange, due to the risks and the ‘substantial additional’ regulatory burden imposed on FSRA, the Applicant/Recognised Investment Exchange will be subject, pursuant to FEES Rules 1.2.5 and 3.14.1(b), an additional fee of $125,000 for the application only.