CRYPTO-ASSET MODULE

MODULE:	CRA (Crypto-asset)

Table of Contents

			Date Last Changed
CRA-A	**Introduction**		
	CRA-A.1	Purpose	xx/2023
	CRA-A.2	Module History	xx/2023
CRA-B	**Scope of Application**		
	CRA-B.1	Overview	xx/2023
CRA-1	**Licensing**		
	CRA-1.1	Crypto Asset Service License	xx/2023
	CRA-1.2	Application for License	xx/2023
	CRA-1.3	Cancellation or Amendment of License	xx/2023
	CRA-1.4	Publication of the Decision to Grant, Cancel or Amend a License	xx/2023
	CRA-1.5	License Application Fees	xx/2023
	CRA-1.6	Annual License Fees	xx/2023
	CRA-1.7	Approved Person	xx/2023
CRA-2	**Licensing Condition**		
	CRA-2.1	Condition 1: Legal Status	xx/2023
	CRA-2.2	Condition 2: Mind and Management	xx/2023
	CRA-2.3	Condition 3: Substantial Shareholders	02/2019
	CRA-2.4	Condition 4: Board and Employees	xx/2023
	CRA-2.5	Condition 5: Financial Resources	xx/2023
	CRA-2.6	Condition 6: Systems and Controls	xx/2023
	CRA-2.7	Condition 7: External Auditor	xx/2023
	CRA-2.8	Condition 8: Other Requirements	xx/2023
CRA-3	**Minimum Capital Requirement**		
	CRA-3.1	General Requirements	xx/2023
	CRA-3.2	Key Requirements	xx/2023
	CRA-3.3	Additional Requirements	02/2019
CRA-4	**Business Standards and Ongoing Obligations**		
	CRA-4.1	General Obligations	xx/2023
	CRA-4.2	Auditors and Accounting Standards	xx/2023
	CRA-4.3	Listing of Crypto-assets	xx/2023
	CRA-4.4	Dealing with Clients	xx/2023
	CRA-4.5	Client Protection	xx/2023
	CRA-4.6	Marketing and Promotion	xx/2023
	CRA-4.7	Complaints	xx/2023

			Date Last Changed
	CRA-4.8	Professional Indemnity Coverage	xx/2023
	CRA-4.9	Other Obligations	xx/2023
	CRA-4.10	Matters Requiring Approval of the CBB	xx/2023
	CRA-4.11	Compliance	xx/2023
	CRA-4.12	Additional Requirements Applicable to licensed crypto-asset exchanges	xx/2023
CRA-5	**Technology Governance and Cyber Security**		
	CRA-5.1	General Requirements	xx/2023
	CRA-5.2	Maintenance and Development of Systems	xx/2023
	CRA-5.3	Security Measures and Procedures	xx/2023
	CRA-5.4	Cryptographic Keys and Wallet Storage	xx/2023
	CRA-5.5	Origin and Destination of crypto-assets	xx/2023
	CRA-5.6	Planned and Unplanned System Outages	02/2019
	CRA-5.7	[This Section has been deleted]	xx/2023
	CRA-5.8	Cyber Security	xx/2023
CRA-6	**Risk Management**		
	CRA-6.1	Board of Directors' Responsibilities	xx/2023
	CRA-6.2	Counterparty Risk	xx/2023
	CRA-6.3	Market Risk	xx/2023
	CRA-6.4	Liquidity Risk	xx/2023
	CRA-6.5	Operational Risk	xx/2023
	CRA-6.6	Outsourcing Risk	07/2022
CRA-7	**[This Chapter has been deleted in xx/2023]**		
	CRA-7.1	[This Section has been deleted]	xx/2023
CRA-8	**Crypto-asset Custody Services**		
	CRA-8.1	General Requirements	xx/2023
	CRA-8.2	Custodial Arrangements	xx/2023
	CRA-8.3	Crypto Wallets	xx/2023
	CRA-8.4	Reconciliation, Client Reporting and Record Keeping	xx/2023
CRA-9	**[This Chapter has been deleted in xx/2023]**		
CRA-10	**Reporting, Notifications and Approvals**		
	CRA-10.1	Reporting Requirements	xx/2023
	CRA-10.2	Notification Requirements	xx/2023
	CRA-10.3	Approval Requirements	xx/2023

			Date Last Changed
CRA-11	**Information Gathering by the CBB**		
	CRA-11.1	Power to Request Information	xx/2023
	CRA-11.2	Access to Premises	xx/2023
	CRA-11.3	Accuracy of Information	xx/2023
	CRA-11.4	Methods of Information Gathering	xx/2023
	CRA-11.5	The Role of the Approved Expert	xx/2023
CRA-12	**Conduct of Business Obligations**		
	CRA-12.1	General Scope and Application	02/2019
	CRA-12.2	Conflict of Interest	xx/2023
	CRA-12.3	Sale Processes and Selling Practices	xx/2023
	CRA-12.4	Accepting Client and Contractual Agreement wit Client	xx/2023
	CRA-12.5	Execution of Clients' Orders	xx/2023
CRA-13	**Prevention of Market Abuse and Manipulation**		
	CRA-13.1	General Requirements	xx/2023
	CRA-13.2	[This Section has been deleted]	xx/2023
	CRA-13.3	[This Section has been deleted]	xx/2023
	CRA-13.4	[This Section has been deleted]	xx/2023
	CRA-13.5	[This Section has been deleted]	xx/2023
	CRA-13.6	[This Section has been deleted]	xx/2023
	CRA-13.7	[This Section has been deleted]	xx/2023
	CRA-13.8	[This Section has been deleted]	xx/2023
	CRA-13.9	[This Section has been deleted]	xx/2023
CRA-14	**[This Chapter has been deleted in xx/2023]**		
	CRA-14.1	[This Section has been deleted]	xx/2023
	CRA-14.2	[This Section has been deleted]	xx/2023
	CRA-14.3	[This Section has been deleted]	xx/2023
	CRA-14.4	[This Section has been deleted]	xx/2023
	CRA-14.5	[This Section has been deleted]	xx/2023
	CRA-14.6	[This Section has been deleted]	xx/2023
	CRA-14.7	[This Section has been deleted]	xx/2023
	CRA-14.8	[This Section has been deleted]	xx/2023
	CRA-14.9	[This Section has been deleted]	xx/2023
	CRA-14.10	[This Section has been deleted]	xx/2023
	APPENDICES		
	Appendix-1	Deleted	xx/2023
	Appendix-2	Deleted	xx/2023
CRA-15	**Digital Tokens**		
	CRA-15.1	Digital Token Offerings	xx/2023
	CRA-15.2	Digital Tokens Issuers Obligations	xx/2023

MODULE	CRA (Crypto-asset)
	Table of Contents (continued)

		Date Last Changed
CRA-15.3	Role and Responsibilities of Digital Token Advisor	xx/2023
CRA-15.4	Trading and Settlement of Digital Tokens	xx/2023

CRA-A.1 Purpose

Executive Summary

CRA-A.1.1 The purpose of this Module is to provide the CBB's Directive concerning trading, dealing, advisory services, portfolio management services in crypto-assets as principal, as agent, as custodian and as a crypto-asset exchange within or from the Kingdom of Bahrain. The key requirements relevant to these activities are outlined in this Module while the licensees are also subject to other relevant Modules of the CBB Rulebook Volume 6. This Directive is supported by Article 44(c) of the Central Bank of Bahrain ('CBB') and Financial Institutions Law (Decree No. 64 of 2006) ('CBB Law').

CRA-A.1.2 This Module must be read in conjunction with other parts of the Rulebook, mainly:

a) [This Subparagraph was deleted in 2023].
b) High-level Controls (corporate governance);
c) Market Intermediaries and Representatives;
d) Anti-Money Laundering and Combating Financial Crime;
e) Dispute Resolution, Arbitration and Disciplinary Proceedings;
f) International Cooperation and Exchange of Information;
g) Market Surveillance, Investigation & Enforcement;
h) Prohibition of Market Abuse and Manipulation; and
i) Training and Competency.

Legal Basis

CRA-A.1.3 **This Module contains the CBB's Directive (as amended from time-to-time) relating to licensees providing regulated crypto-asset services (henceforth referred to as licensees) as defined in the Rulebook and is issued under the powers available to the CBB under Article 38 of the CBB Law. Licensees must also comply with the relevant Modules of the Rulebook Volume 6.**

CRA-A.1.4 For an explanation of the CBB's Rule-making powers and different regulatory instruments, see Section UG-1.1.

CRA-A.2 Module History

CRA-A.2.1 This Module was first issued in February 2019. Changes made subsequently to this Module are annotated with the calendar quarter date in which the change was made as detailed in the table below. Chapter UG 3 provides further details on Rulebook maintenance and version control.

Module Ref.	Change Date	Description of Changes
CRA-1.1.6(f)	04/2019	Amended sub-paragraph.
CRA-1.1.6(g)	04/2019	Moved to sub-paragraph (f).
CRA-1.6.3	04/2019	Added License fee table based on Category.
CRA-1.6.10	04/2019	Amended Paragraph.
CRA-B.1	01/2020	Added reference to cyber security risk.
CRA-4.1.1	01/2020	Amended reference to CRA-4.1.1 (r).
CRA-5.2.6-CRA-5.2.9	01/2020	Added new Paragraphs on the requirements of IT System Audit.
CRA-5.3.6	01/2020	Removed "at least annually" for security tests.
CRA-5.8	01/2020	Added these terms: Cyber Security Risk, Cyber Security Incident, Cyber Security Threats.
CRA-5.8.19A	01/2020	Added a new Paragraph on requirements to submit a comprehensive report on cyber security incident.
CRA-5.8.24	01/2020	Deleted Paragraph.
CRA-5.8.25	01/2020	Deleted Paragraph.
CRA-5.8.25A	01/2020	Added a new Paragraph on requirements for periodic assessments of cyber security threats.
CRA-5.8.28 - CRA-5.8.29	01/2020	Added new Paragraphs on the requirement for cyber security insurance.
CRA-7.1.1	01/2020	Amended Paragraph.
CRA-7.1.1A	01/2020	Added a new Paragraph on references to Module AML.
CRA-7.1.2	01/2020	Deleted Paragraph.
CRA-7.1.3	01/2020	Added clarification that simplified customer due diligence is not allowed.
CRA-7.1.5	01/2020	Added a new Paragraph on reference to Module AML and removed transaction record details.
Appendix-1	01/2020	Added reference to cyber security incident.
Appendix-2	01/2020	Amended Mitigation and aggravating factors.
CRA-4.1.1A	10/2020	Added a new Paragraph on Provision of Financial Services on a Non-discriminatory Basis.
CRA-10.1.9	01/2022	Amended Paragraph on the submission of the written assessment of the observations/issues raised in the Inspection draft report.
CRA-10.3.1	01/2022	Amended Paragraph on change in licensee corporate and legal name.
CRA-10.3.2	01/2022	Amended Paragraph on change in licensee legal name.
CRA-6.6	07/2022	Replaced Section with new Outsourcing Requirements.
CRA	XX/2023	Amended Module including a new Chapter on Digital Token Offerings and enhancements to cyber security requirements.

Effective Date

CRA-A.2.2 **The contents of this Module are effective from the date of release of the Module or the changes to the Module unless specified otherwise.**

CRA-B.1 Overview

CRA-B.1.1 The CBB has recognised that the market for crypto-assets has been growing globally and people around the world and in Bahrain are currently dealing, buying, selling or otherwise holding positions in crypto-assets. The CBB's Rules are aimed at minimising the risk and, in particular, the risk of financial crime and illegal use of crypto-assets.

CRA-B.1.2 The Rules contained in this Directive cover licensing requirements, the conditions for the issuance and holding the CBB license, minimum capital requirements, measures to safeguard client or customer interests, technology standards and in particular the cyber security risk management requirements, reporting, notifications and approval requirements, conduct of business obligations, prevention of market abuse and manipulation, enforcement and the powers under the CBB Law for inspections and access.

CRA-B.1.3 The Rules additionally cover the regulatory framework governing the offerings of digital tokens in/from the Kingdom of Bahrain. Pursuant to the authority of the CBB under Article (1) (definition of "securities") of the CBB Law, digital tokens issued pursuant to this Module are considered as securities.

CRA-B.1.4 Digital tokens have the potential to spur innovation and efficiency in capital raising or as investment opportunity and, as a result, the market for digital token has been growing at a rapid pace. While digital tokens may present a new way to raise capital, they also bring increased risk due to the underlying technologies upon which they are structured. Digital token offerings necessitate the classification of every offering as a security or otherwise, based on the features of the digital token.

CRA-B.1.5 **Chapters CRA-1 to CRA-14 apply to Category 1, 2, 3 and 4 licensees offering regulated crypto-asset services. Chapter CRA-15 contains applicable rules on digital tokens and the requirements applicable to digital token advisors and digital token issuers. The rules contained in Chapters CRA-1 to CRA-14 are not applicable to digital token issuers.**

CRA-B.1.6 **A person that contravenes the provisions of this Module or other applicable Modules of the CBB Rulebook may be subject to enforcement actions in accordance with the provisions of the CBB Law.**

MODULE	CRA: Crypto-asset
CHAPTER	CRA-1 Licensing

CRA-1.1 License for crypto-asset service

CRA-1.1.1 **No person may market or undertake the activities, by way of business, within or from the Kingdom of Bahrain, comprised of regulated crypto-asset services without obtaining a license from the CBB.**

CRA-1.1.2 **For the purposes of Paragraph 1.1.1, undertake the activities, by way of business means:**

(a) Providing one or more of services specified in Paragraph CRA-1.1.6 for commercial gain;

(b) Holding oneself out as willing and able to provide the services specified in Paragraph CRA-1.1.6; or

(c) Regularly soliciting other persons to engage in providing the services specified in Paragraph CRA-1.1.6.

CRA-1.1.3 [This Paragraph was deleted in XX 2023].

CRA-1.1.4 For the purpose of this Module, any promotion, offering, announcement, advertising, broadcast or any other means of communication made for the purpose of inducing recipients to purchase, exchange, or otherwise acquire financial services in return for monetary payment or some other form of valuable consideration shall be considered "marketing" in accordance with Resolution No. (16) for the year 2012.

CRA-1.1.5 The activities will be deemed to be undertaken 'within or from the Kingdom of Bahrain', if, for example, the person concerned:

(a) Is incorporated in the Kingdom of Bahrain;

(b) Uses an address situated in the Kingdom of Bahrain for its correspondence; or

(c) Directly solicits clients within the Kingdom of Bahrain.

CRA-1.1 License for crypto-asset service (continued)

Regulated Crypto-Asset Services

CRA-1.1.6 Regulated crypto-asset services means the conduct of any or any combination of the following types of activities:

(a) Reception and Transmission of order: The reception from a client of an order to buy and/or sell one or more crypto-assets and the transmission of that order to a third party for execution.

(b) Trading in crypto-assets as agent: Acting to conclude agreements to buy and/or sell for one or more crypto-assets on behalf of the clients.

(c) Trading in crypto-assets as principal: Trading against proprietary capital resulting in conclusion of transactions in one or more crypto-assets.

(d) Portfolio Management: Managing crypto-assets belonging to a client and the arrangement for their management are such that the licensee managing those crypto-assets has a discretion to invest in one or more crypto-assets.

(e) Crypto-asset Custodian: safeguarding, storing, holding, maintaining custody of or arranging on behalf of clients for crypto-assets.

(f) Investment Advice: Giving or offering, to persons in their capacity as investors or potential investors or as agent for an investors or potential investor, a personal recommendation in respect of one or more transactions relating to one or more crypto-assets. A "personal recommendation" means a recommendation presented as suitable for the client to whom it is addressed, or which is based on a consideration of the circumstances of that person, and must constitute a recommendation to buy, sell, exchange, exercise or not to exercise any right conferred by a particular crypto-asset, or hold a particular crypto-asset.

(g) [This subparagraph was moved to CRA-1.1.6(f) in April 2019].

CRA-1.1 License for crypto-asset service (continued)

(h) Crypto-asset exchange: means a crypto-asset exchange, licensed by the CBB and operating in or from the Kingdom of Bahrain, on which trading, conversion or exchange of:
(i) crypto-assets for fiat currency or vice versa; and/or
(ii) crypto-assets for another crypto-asset,
may be transacted in accordance with the Rules of the crypto-asset exchange.

(i) Digital token advisor: advise and guide a digital token issuer on all matters relating to offering of digital tokens, trading of digital tokens as well as on the responsibilities and obligations of the digital token issuer pursuant to the provisions of applicable law, rules and regulations.

CRA-1.1.6A Licensees intending to offer regulated crypto-asset services which were not included in its application for licence and/or additional services which are not part of the regulated crypto-asset services specified in Paragraph CRA-1.1.6, must seek the CBB's prior written approval before offering the service. Licensees must provide the CBB with detailed description of the new services, the resources required and the operational framework for such service.

Exclusions

CRA-1.1.7 The following activities do not constitute regulated crypto-asset services:
(a) the creation of crypto assets;
(b) the development, dissemination or use of software for the purpose of creating or mining a crypto asset;
(c) a loyalty programme; or
(d) any other activity or arrangement that is deemed by the CBB to not constitute undertaking regulated crypto-asset services.

CRA-1.1.8 Depending on the type of regulated crypto-asset services that a person wishes to undertake, applicants may seek to be licensed by the CBB under one of the following 4 categories of license:

CRA-1.1 License for crypto-asset service (continued)

Category 1

CRA-1.1.9 Category 1 licensees may undertake one or more regulated crypto-asset service, as listed below:
(a) Reception and transmission of orders;
(b) Provide investment advice in relation to crypto-assets.

CRA-1.1.10 When undertaking the regulated crypto-asset services listed under Rule CRA- 1.1.9, Category 1 licensees:
(a) Must not hold any client assets or client money;
(b) Must refrain from receiving any fees or commissions from any party other than the client; and
(c) Must not operate a crypto-asset exchange.

Category 2

CRA-1.1.11 Category 2 licensees may undertake one or more regulated crypto-asset services, as listed below:
(a) Trading in crypto-assets as agent;
(b) Portfolio Management;
(c) Crypto-asset custody;
(d) Investment advice.

CRA-1.1.12 When undertaking the regulated crypto-asset services listed under Rule CRA- 1.1.11, Category 2 licensees may hold or control client asset and client money but must not deal from their own account ("dealing as principal") or operate a crypto-asset exchange.

Category 3

CRA-1.1.13 Category 3 licensees may undertake one or more regulated crypto-asset services, as listed below:
(a) Trading in crypto-assets as agent;
(b) Trading in crypto-assets as principal;
(c) Portfolio Management;
(d) Crypto-asset custody;
(e) Investment advice;
(f) To act as a digital token advisor.

CRA-1.1 License for crypto-asset service (continued)

CRA-1.1.14 When undertaking regulated crypto-asset services listed under Rule CRA-1.1.13, Category-3 licensees may hold or control client assets and client money, may deal on their own account ("dealing as principal") but must not operate a crypto-asset exchange.

Category 4

CRA-1.1.15 Category 4 licensees may undertake one or more regulated crypto-asset service, as listed below:

(a) Operate a licensed crypto-asset exchange;

(b) Crypto-asset custody service;

(c) To act as a digital token advisor.

CRA-1.1.16 Licensees offering crypto-asset exchange service (licensed crypto-asset exchange) must not execute client orders against proprietary capital, or engage in matched principal trading.

CRA-1.1.16A Pursuant to Section CRA-15.4 (Trading and Settlement of Digital Tokens), licensees may undertake over-the-counter trading in digital tokens which are issued in accordance with the requirements of Chapter CRA-15. The requirements of Paragraph CRA-1.1.16 are not applicable to trading in digital tokens provided the CBB has provided the licensee with an approval to trade the digital token under the over-the-counter trading framework.

CRA-1.1.17 When undertaking the regulated crypto-asset services listed under Rule CRA-1.1.15, Category-4 licensees may hold or control client asset and client money.

CRA-1.1.18 Persons wishing to be licensed to undertake the activities of regulated crypto-asset services must apply in writing to the CBB in accordance with the requirements stipulated in CRA-1.2.

CRA-1.1 License for crypto-asset service (continued)

CRA-1.1.19 **[This Paragraph was deleted in XX 2023].**

CRA-1.1.20 [This Paragraph was deleted in XX 2023].

CRA-1.1.21 [This Paragraph was deleted in XX 2023].

CRA-1.1.22 **Applicants seeking a regulated crypto-asset service license must satisfy the CBB that they meet, by the date of grant of license, the minimum criteria for licensing, as contained in Chapter CRA-2. Once licensed, the regulated crypto-asset service licensee must continue to meet these criteria on an on-going basis.**

CRA-1.1.23 [This Paragraph was deleted in XX 2023].

CRA-1.1.24 [This Paragraph was deleted in XX 2023].

CRA-1.1.25 [This Paragraph was deleted in XX 2023].

Differentiation Between Intermediary Activity and Exchange Activity

CRA-1.1.26 **Category-1, Category-2 and Category-3 crypto-asset licensees intending to operate solely as a broker and/or dealer for clients (intermediary service) are not permitted to structure their broking / dealing service or platform in such a way that it would be deemed as operating a market i.e. a crypto asset exchange. The CBB 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.**

CRA-1.1 License for crypto-asset service (continued)

CRA-1.1.27 Category 1, Category 2 and Category 3 crypto-asset licensees should design and structure their 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 licensed crypto asset exchange. In practice, category 1, category 2 and category 3 crypto-asset licensees must not:

(a) Display any publicly-accessible information that may appear like a trading order book;

(b) Provide for any price discovery; and

(c) Give actual or potential clients the impression that they are interacting with a licensed crypto-asset exchange.

CRA-1.2 Application for License

CRA-1.2.1 **Applicants for a license must submit a duly completed Form 1 (Application for a License), under cover of a letter signed by an authorised signatory of the applicant marked for the attention of the Director, Licensing Directorate. The application must be accompanied by the documents listed in Rule CRA-1.2.4, unless otherwise directed by the CBB.**

CRA-1.2.2 [This Paragraph was deleted in XX 2023]

CRA-1.2.3 References to applicant mean the proposed licensee seeking a license. An applicant may appoint a representative – such as a law firm or professional consultancy – to prepare and submit the application. However, the applicant retains full responsibility for the accuracy and completeness of the application, and is required to certify the application form accordingly. The CBB also expects to be able to liaise directly with the applicant during the licensing process, when seeking clarification of any issues.

CRA-1.2.4 **Unless otherwise directed by the CBB, the following documents must be provided in support of the application for license:**

(a) A duly completed Form 2 (Application for Authorisation of Shareholders) for each Shareholder of the proposed licensee;

(b) A duly completed Form 3 (Application for Approved Person status), for each individual proposed to undertake a controlled function (as defined in Rule CRA-1.7.2) in the proposed licensee;

(c) A comprehensive business plan for the application, addressing the matters described in Rule CRA-1.2.6;

(d) [This Sub-Paragraph was deleted in XX 2023].

(e) A copy of the applicant's commercial registration certificate;

(f) A certified copy of a Board resolution of the applicant, confirming its decision to seek a CBB crypto-asset service license;

CRA-1.2 Application for License (continued)

(g) In the case of applicants that are part of a group, a letter of non-objection to the proposed license application from the applicant's lead supervisor, together with confirmation that the group is in good regulatory standing and is in compliance with applicable supervisory requirements, including those relating to capital requirements;

(h) [This Sub-Paragraph was deleted in XX 2023].

(i) [This Sub-Paragraph was deleted in XX 2023].

(j) In the case of applicants that are part of a group, copies of the audited financial statements of the applicant's group, for the three years immediately prior to the date of application;

(k) In the case of applicants not falling under (j) above, copies of the audited financial statements of the applicant's substantial shareholder (where they are a legal person), for the three years immediately prior to the date of application; and

(l) A copy of the applicant's memorandum and articles of association (in draft form for applicants creating a new company).

(m) [This Sub-Paragraph was deleted in XX 2023].

CRA-1.2.5 The CBB, in its complete discretion may ask for a letter of guarantee from the applicant's controlling or major shareholders on a case by case basis as it deems appropriate/necessary as part of the required documents to be submitted pursuant to Paragraph CRA-1.2.4 above.

CRA-1.2 Application for License (continued)

CRA-1.2.6 The business plan submitted in support of an application must include:

(a) An outline of the history of the applicant and its shareholders including the Ultimate Beneficiary Owners (UBO);

(b) A description of the proposed, current, and historical business of the applicant, including detail on the products and services provided and to be provided, all associated websites addresses, the jurisdictions in which the applicant is engaged in business, the principal place of business, the primary market of operation and the projected customer base;

(c) The reasons for applying for a license, including the applicant's strategy and market objectives;

(cc) Details of the KYC and customer on-boarding process;

(d) The proposed Board and senior management of the applicant and the proposed organisational structure of the applicant along with the proposed organization chart and the reporting lines;

(dd) Detailed full business cycle flow from end to end of the business model;

(e) An assessment of the risks that may be faced by the applicant, together with the proposed systems and controls framework to be put in place for addressing those risks and to be used for the main business functions;

(f) An opening balance sheet for the applicant, together with a three-year financial projection, with all assumptions clearly outlined, demonstrating that the applicant will be able to meet applicable capital adequacy requirements;

(g) Details of all banking arrangements for fund transfer as well as any other alternative form of arrangements for transfer of funds;

(h) A copy of its business continuity plan; and

(i) A description of the IT system that will be used, including details of how the IT system and other records will be backed up.

CRA-1.2 Application for License (continued)

CRA-1.2.7 **The applicant's memorandum and articles of association must explicitly provide for it to undertake the activities proposed in the license application, and must preclude the applicant from undertaking other regulated services, or commercial activities, unless these arise out of its regulated crypto-asset services or are incidental to those.**

CRA-1.2.8 **All documentation provided to the CBB as part of an application for a license must be in either the Arabic or English languages. Any documentation in a language other than English or Arabic must be accompanied by a certified English or Arabic translation thereof.**

CRA-1.2.9 **Any material changes or proposed changes to the information provided to the CBB in support of a licensing application that occurs prior to licensing must be reported to the CBB.**

CRA-1.2.10 Failure to inform the CBB of the changes specified in Rule CRA-1.2.9 is likely to be viewed as a failure to provide full and transparent disclosure of information, and thus a failure to meet licensing condition stipulated in Paragraph CRA-2.8.2.

Licensing Process and Timelines

CRA-1.2.11 Articles 44 to 47 of the CBB Law govern the licensing process which stipulate that the CBB will issue its decision within 60 calendar days of an application being deemed complete (i.e. containing all required information and documents). By law, the 60 days' time limit only applies once the application is complete and all required information (which may include any clarifications requested by the CBB) and documents have been provided. This means that all the items specified in Rule CRA-1.2.4 have to be provided, before the CBB may issue a license.

CRA-1.2.12 The CBB recognises, however, that applicants may find it difficult to secure suitable senior management (refer CRA-1.2.4(b) above) in the absence of preliminary assurances regarding the likelihood of obtaining a license.

CRA-1.2 Application for License (continued)

CRA-1.2.13 [This Paragraph was deleted in XX 2023].

CRA-1.2.14 [This Paragraph was deleted in XX 2023].

CRA-1.2.15 [This Paragraph was deleted in XX 2023].

CRA-1.2.16 Therefore, all potential applicants are strongly encouraged to contact the CBB at an early stage to discuss their plans, for guidance on the CBB's license categories and associated requirements. The Licensing Directorate would normally expect to hold at least one pre-application meeting with an applicant, prior to receiving an application.

CRA-1.2.17 Potential applicants should initiate pre-application meetings in writing, setting out a short summary of their proposed business and any issues or questions that they may have already identified, once they have a clear business proposition in mind and have undertaken their preliminary research. The CBB can then guide the applicant on the specific areas in the Rulebook that will apply to them and the relevant requirements that they must address in their application.

CRA-1.2 Application for License (continued)

CRA-1.2.18 **An applicant must not hold himself out as having been licensed by the CBB, prior to the issuance of the CBB's Resolution on granting the license. Failure to do so may constitute grounds for refusing an application and result in a contravention of Article 42 of the CBB Law (which carries a maximum penalty of BD 1 million).**

Granting or Refusal of License

CRA-1.2.19 Should a license be granted, the CBB will notify the applicant in writing of the fact; the CBB will also publish its decision to grant a license in the Official Gazette and in two local newspapers (one published in Arabic, the other in English). The license may be subject to such terms and conditions as the CBB deems necessary for the additional conditions being met.

CRA-1.2.20 The CBB may reject an application for a license if in its opinion:

(a) The requirements of the CBB Law or the Rulebook are not met;
(b) False or misleading information has been provided to the CBB, or information which should have been provided to the CBB has not been so provided; or
(c) The CBB believes it necessary in order to safeguard the interests of potential clients.

CRA-1.2.21 Where the CBB intends to refuse an application for a license, it must give the applicant written notice to that effect. Applicants will be given a minimum of 30 calendar days from the date of the written notice to appeal the decision, as per the appeal procedures specified in the notice.

CRA-1.2.22 **Before the final approval is granted to a licensee, a confirmation from a retail bank addressed to the CBB that the minimum capital, as specified in this Module, has been paid in must be provided to the CBB.**

CRA-1.2 Application for License (continued)

Readiness Assessment

CRA-1.2.23 **Prior to commencement of operation, a licensee must, after obtaining the CBB's prior written approval, appoint an independent third party to undertake a readiness assessment and submit a readiness assessment report.**

CRA-1.2.24 **The readiness assessment report must include the licensee's risk management system, capital adequacy, organisational structure, operational manuals, information technology, information system security, policies and procedures and internal controls and systems.**

CRA-1.2.25 [This Paragraph was deleted in XX 2023].

Commencement of Operations

CRA-1.2.26 **Prior to commencement of operation the new licensee must provide to the CBB (if not previously submitted):**

(a) The registered office address and details of premises to be used to carry out the business of the proposed licensee;
(b) [This Sub-paragraph was deleted in XX 2023];
(c) The licensee's contact details including telephone and fax number, e-mail address and website;
(d) [This Sub-paragraph was deleted in XX 2023];
(e) [This Sub-paragraph was deleted in XX 2023];
(f) A copy of the auditor's acceptance to act as auditor for the applicant;
(g) A certificate from a retail bank operating in Bahrain certifying that the capital is deposited;

CRA-1.2 Application for License (continued)

(h) A copy of the licensee's professional indemnity insurance policy;
(i) A copy of the applicant's notarized memorandum and articles of association, addressing the matters described in Paragraph CRA-1.2.9;
(j) A copy of the commercial registration certificate in Arabic and in English from the Ministry of Commerce, Industry and Tourism;
(k) [This Sub-paragraph was deleted in XX 2023];
(l) Any other information as may be specified by the CBB;
(m) A written confirmation, addressed to the CBB, from a licensed retail bank, stating that necessary banking arrangements, including opening of accounts (both corporate account and client money account) has been made by the applicant; and
(n) Where the licensee has entered into an agreement with a third party, other than a licensed bank, for the purpose of transfer of funds, a copy of the written agreement between the licensee and the third party.

CRA-1.2.27 Licensees must commence their commercial operations within 6 months of being granted a license by the CBB, failing which the CBB may cancel the license, in accordance with the provisions of the CBB Law.

CRA-1.2.28 [This Paragraph was deleted in XX 2023].

CRA-1.3 Cancellation or Amendment of License

Voluntary Surrender of a License

CRA-1.3.1 **In accordance with Article 50 of the CBB Law, licensees wishing to cease carrying out all the approved regulated services, must obtain the CBB's written approval, before ceasing their activities. All such requests must be made in writing to the Director, Capital Markets Supervision, setting out in full the reasons for the request and how the business is to be wound up.**

CRA-1.3.2 **Licensees must satisfy the CBB that their clients' interests are to be safeguarded during and after the proposed cancellation.**

CRA-1.3.3 The CBB will approve a request for cancellation of license by a licensee where there is no outstanding regulatory concerns and client interests would not be prejudiced. A voluntary surrender will only be allowed to take effect once the licensee, in the opinion of the CBB, has discharged all its regulatory obligations towards clients.

Cancellation of a License by the CBB

CRA-1.3.4 Pursuant to Article 48 (c) of the CBB Law, the CBB may cancel a license, for instance if a licensee fails to satisfy any of its existing license conditions or in order to protect the legitimate interests of clients or creditors of the licensee. The CBB generally views the cancellation of a license as appropriate only in the most serious of circumstances, and generally tries to address supervisory concerns through other means beforehand.

CRA-1.3.5 The procedures for cancellation of a license are contained in Articles 48 and 49 of the CBB Law.

CRA-1.3 Cancellation or Amendment of License (continued)

CRA-1.3.6 The CBB will only effect the cancellation once a licensee has discharged all its regulatory responsibilities to clients. Until such time, the CBB will retain all its regulatory powers towards the licensee and will direct the licensee so that no new regulated crypto-asset services may be undertaken whilst the licensee discharges its obligations to its clients.

Amendment to the scope of regulated services under the license or Amendment of the license

CRA-1.3.7 **Licensees wishing to vary the scope of the regulated services under their existing license, whether by adding or ceasing some services, must obtain the CBB's prior written approval. The CBB's prior written approval must also be sought in relation to an amendment to the licensee's license category.**

CRA-1.4 Publication of the Decision to Grant, Cancel or Amend a License

CRA-1.4.1 In accordance with Articles 47 and 49 of the CBB Law, the CBB must publish its decision to grant, cancel or amend a license in the Official Gazette and in two local newspapers, one in Arabic and the other in English.

CRA-1.4.2 **For the purposes of Paragraph CRA-1.4.1, the cost of publication must be borne by the Licensee.**

CRA-1.4.3 The CBB may also publish its decision on such cancellation or amendment using any other means it considers appropriate, including electronic means.

CRA-1.5 Licensing Application Fees

CRA-1.5.1 **Applicants seeking a regulated crypto-asset service license from the CBB must pay a non-refundable license application fee of BD 100 at the time of submitting their formal application to the CBB.**

CRA-1.5.2 [This Paragraph was deleted in XX 2023].

CRA-1.6 Annual License Fees

CRA-1.6.1 **Licensees must pay the relevant annual license fee to the CBB, on 1st December of the preceding year for which the fee is due.**

CRA-1.6.2 The relevant fees are specified in Rule CRA-1.6.3 below. The fees due on 1st December are those due for the following calendar year, but are calculated on the basis of the firm's latest audited financial statements for the previous calendar year: i.e. the fee payable on 1st December 2013 for the 2014 year (for example), is calculated using the audited financial statements for 2012, assuming a 31st December year end. Where a licensee does not operate its accounts on a calendar-year basis, then the most recent audited financial statements available are used instead.

CRA-1.6.3 **The variable annual license fee payable by licensees is 0.25% of their relevant operating expenses, subject to a minimum and maximum as per the table below:**

Sl. No.	Licensing Category	Minimum Fees (BD)	Maximum Fees (BD)
1.	Category-1	2,000	6,000
2.	Category-2	3,000	8,000
3.	Category-3	4,000	10,000
4.	Category-4	5,000	12,000

CRA-1.6.4 **Relevant operating expenses are defined as the total operating expenses of the licensee concerned, as recorded in the most recent audited financial statements available, subject to the adjustments specified in Rule CRA-1.6.5.**

CRA-1.6.5 **The adjustments to be made to relevant operating expenses are the exclusion of the following items from total operating expenses:**
(a) Training costs;
(b) Charitable donations;
(c) CBB fees paid; and
(d) Non-executive Directors' remuneration.

CRA-1.6 Annual License Fees (continued)

CRA-1.6.6 For the avoidance of doubt, operating expenses for the purposes of this Section, do not include items such as depreciation, provisions, interest expense, and dividends.

CRA-1.6.7 The CBB would normally rely on the audited accounts of a licensee as representing a true and fair picture of its operating expenses. However, the CBB reserves the right to enquire about the accounting treatment of expenses, and/or policies on intra-group charging, if it believes that these are being used artificially to reduce a license fee.

CRA-1.6.8 **Licensees must complete and submit Form ALF (Annual License Fee) to the CBB, no later than 15th October of the preceding year for which the fees are due.**

CRA-1.6.9 **Licensees are subject to direct debit for the payment of the annual fee and must complete and submit to the CBB a Direct Debit Authorisation Form by 15th September available under Part B of Volume 6 (Capital Markets) CBB Rulebook on the CBB Website.**

CRA-1.6.10 **For new licensees, the first annual license fee is payable when the license is issued by the CBB. The amount payable is the minimum amount stipulated in Paragraph CRA-1.6.3 for each category of license.**

CRA-1.6.11 **For the first full year of operation, the licensee would calculate its fee as the floor amount. For future years, the licensee would submit a Form ALF by 15th October of the preceding year for which the fees are due and calculate its fee using its last audited financial statements (or alternative arrangements as agreed with CBB, should its first set of accounts cover an 18-month period).**

CRA-1.6.12 Where a license is cancelled (whether at the initiative of the firm or the CBB), no refund is paid for any months remaining in the calendar year in question.

CRA-1.6.13 [This Paragraph was deleted in XX 2023].

CRA-1.7 Approved Persons

General Requirements

CRA-1.7.1 **Licensees must obtain the CBB's prior written approval in relation to any person wishing to undertake a controlled function in a licensee. The approval from the CBB must be obtained prior to their appointment.**

CRA-1.7.2 **Controlled functions are those functions occupied by board members and persons in executive positions and include:**

(a) Director;
(b) Chief Executive or General Manager;
(c) Head of function;
(d) Chief Information Security Officer;
(e) Compliance Officer; and
(f) Money Laundering Reporting Officer (MLRO).

CRA-1.7.3 **[This Paragraph was deleted in XX 2023].**

CRA-1.7.4 **[This Paragraph was deleted in XX 2023].**

CRA-1.7.5 The CBB may grant an exemption from appointment of some of the controlled functions contained in Paragraph CRA-1.7.2, provided the licensee appoints at least the following controlled functions (i) Directors, (ii) Chief Executive or General Manager, (iii) Compliance Officer and (iv) Money Laundering Reporting Officer.

CRA-1.7.6 Pursuant to CRA-1.7.5, a licensee seeking exemption from appointment of persons to specific controlled functions should provide in writing to the satisfaction of the CBB:

(a) Nature, scale and complexity of their business and how performance of the controlled function to which no appointment is to be made will be managed;
(b) Provide alternative arrangements which should ensure sound and prudent management and adequate consideration to the interest of clients and the integrity of the market; and
(c) Confirmation that the individual entrusted with additional responsibilities pertaining to a controlled function is of sufficient good repute, possesses sufficient knowledge, skill and experience and ability to commit sufficient time to discharge the additional responsibility.

CRA-1.7 Approved Persons (continued)

Fit and Proper

CRA-1.7.7 Licensees seeking an approved person authorisation for an individual, must satisfy the CBB that the individual concerned is 'fit and proper' to undertake the controlled function in question.

CRA-1.7.8 Each applicant applying for approved person status and those individuals occupying approved person positions must comply with the following conditions:

(a) Has not previously been convicted of any felony or crime that relates to his/her honesty and/or integrity unless he/she has subsequently been restored to good standing;

(b) Has not been the subject of any adverse finding in a civil action by any court or competent jurisdiction, relating to fraud;

(c) Has not been adjudged bankrupt by a court unless a period of 10 years has passed, during which the person has been able to meet all his/her obligations and has achieved economic accomplishments;

(d) Has not been disqualified by a court, regulator or other competent body, as a director or as a manager of a corporation;

(e) Has not failed to satisfy a judgement debt under a court order resulting from a business relationship;

(f) Must have personal integrity, good conduct and reputation;

(g) Has appropriate professional and other qualifications for the controlled function in question. All persons proposed to undertake any controlled functions must meet the relevant examination and qualification requirements of the CBB.; and

(h) Has sufficient experience to perform the duties of the controlled function.

CRA-1.7 Approved Persons (continued)

CRA-1.7.8A In assessing the conditions prescribed in Paragraph CRA-1.7.8, the CBB will take into account the criteria contained in Paragraph CRA-1.7.8B. The CBB reviews each application on a case-by-case basis, taking into account all relevant circumstances. A person may be considered 'fit and proper' to undertake one type of controlled function but not another, depending on the function's job size and required levels of experience and expertise. Similarly, a person approved to undertake a controlled function with a licensee may not be considered to have sufficient expertise and experience to undertake nominally the same controlled function but in a much bigger licensee.

CRA-1.7.8B In assessing a person's fitness and propriety, the CBB will also consider previous professional and personal conduct (in Bahrain or elsewhere) including, but not limited to, the following:

(a) The propriety of a person's conduct, whether or not such conduct resulted in a criminal offence being committed, the contravention of a law or regulation, or the institution of legal or disciplinary proceedings;
(b) A conviction or finding of guilt in respect of any offence, other than a minor traffic offence, by any court or competent jurisdiction;
(c) Any adverse finding in a civil action by any court or competent jurisdiction, relating to misfeasance or other misconduct in connection with the formation or management of a corporation or partnership;
(d) Whether the person, or anybody corporate, partnership or unincorporated institution to which the applicant has, or has been associated with as a director, controller, manager or company secretary been the subject of any disciplinary proceeding, investigation or fines by any government authority, regulatory agency or professional body or association;
(e) The contravention of any financial services legislation;
(f) Whether the person has ever been refused a license, authorisation, registration or other authority;
(g) Dismissal or a request to resign from any office or employment;
(h) Whether the person has been a Director, partner or manager of a corporation or partnership which has gone into liquidation or administration or where one or more partners have been declared bankrupt whilst the person was connected with that partnership;
(i) The extent to which the person has been truthful and open with supervisors; and
(j) Whether the person has ever entered into any arrangement with creditors in relation to the inability to pay due debts.

CRA-1.7 Approved Persons (continued)

CRA-1.7.8C With respect to Paragraph CRA1.7.8B, the CBB will take into account the length of time since any such event occurred, as well as the seriousness of the matter in question.

CRA-1.7.8D **Approved persons undertaking a controlled function must act prudently, and with honesty, integrity, care, skill and due diligence in the performance of their duties. They must avoid any conflict of interest arising whilst undertaking a controlled function.**

CRA-1.7.8E In determining where there may be a conflict of interest arising, factors that may be considered will include whether:

(a) A person has breached any fiduciary obligations to the licensee or terms of employment;

(b) A person has undertaken actions that would be difficult to defend, when looked at objectively, as being in the interest of the licensee and its clients; and

(c) A person has failed to declare a personal interest that has a material impact in terms of the person's relationship with the licensee.

Prior Approval Requirements and Process

CRA-1.7.8F **An application for approval for a person occupying a controlled function under Paragraph CRA-1.7.2 must be made by submitting to the CBB a duly completed Form 3 (Application for Approved Person Status) and Curriculum Vitae after verifying that the information in the Form 3, including previous experience is accurate. Form 3 is available under Volume 6 Part B Authorisation Forms CRA Forms of the CBB Rulebook.**

CRA-1.7 Approved Persons (continued)

CRA-1.7.8G **When the request for approved person status forms part of a license application, it must be marked for the attention of the Director, Licensing and Policy Directorate. When the submission to undertake a controlled function is in relation to an existing licensee, except if dealing with a MLRO, it must be marked for the attention of the Director, Capital Markets Supervision Directorate. In case of the MLRO, Form 3 must be marked for the attention of the Director, Compliance Directorate.**

CRA-1.7.8H **When submitting the Forms 3, licensees must ensure that the Form 3 is:**

(a) Submitted to the CBB with a covering letter signed by an authorised representative of the licensee, seeking CBB approval;

(b) Submitted in original form;

(c) Submitted with a certified copy of the applicant's passport, original or certified copies of educational and professional qualification certificates (and translation if not in Arabic or English) and the Curriculum Vitae; and

(d) Signed by an authorised representative of the licensee and all pages stamped with the licensee's seal.

CRA-1.7.8I **Licensees seeking to appoint Board Directors must seek CBB approval for all the candidates to be put forward for election/approval at a shareholders' meeting, in advance of the agenda being issued to shareholders. CBB approval of the candidates does not in any way limit shareholders' rights to refuse those put forward for election/approval.**

CRA-1.7.8J For existing licensees applying for the appointment of a Director or the Chief Executive/General Manager, the authorised representative should be the Chairman of the Board or a Director signing on behalf of the Board. For all other controlled functions, the authorised representative should be the Chief Executive/General Manager.

CRA-1.7 Approved Persons (continued)

Assessment of Application

CRA-1.7.8K The CBB shall review and assess the application for approved person status to ensure that it satisfies all the conditions required in Paragraph CRA-1.7.8 and the criteria outlined in Paragraph CRA-1.7.8B.

CRA-1.7.8L For purposes of Paragraph CRA-1.7.8I, licensees should give the CBB a reasonable amount of notice in order for an application to be reviewed. The CBB shall respond within 15 business days from the date of meeting all required conditions and regulatory requirements, including but not limited to, receiving the application complete with all the required information and documents, as well as verifying references.

CRA-1.7.8M The CBB reserves the right to refuse an application for approved person status if it does not satisfy the conditions provided for in Paragraph CRA-1.7.8 and the criteria outlined in Paragraph CRA-1.7.8B. A notice of such refusal is issued to the licensee concerned, setting out the basis for the decision.

Appeal Process

CRA-1.7.8N Licensee or the nominated approved persons may, within 30 calendar days of the notification, appeal against the CBB's decision to refuse the application for approved person status. The CBB shall decide on the appeal and notify the licensee of its decision within 30 calendar days from submitting the appeal.

CRA-1.7.8O Where notification of the CBB's decision to grant a person approved person status is not issued within 15 business days from the date of meeting all required conditions and regulatory requirements, including but not limited to, receiving the application complete with all the required information and documents, licensees or the nominated approved persons may appeal to the Executive Director, Financial Institutions Supervision of the CBB provided that the appeal is justified with supporting documents. The CBB shall decide on the appeal and notify the licensee of its decision within 30 calendar days from the date of submitting the appeal.

CRA-1.7 Approved Persons (continued)

Notification Requirements and Process

CRA-1.7.9 **Licensees must promptly notify the CBB in writing when a person undertaking a controlled function will no longer be carrying out that function together with an explanation as to the reasons for not undertaking the controlled function. In such cases, their approved person status is automatically withdrawn by the CBB. If a controlled function falls vacant, the licensee must appoint a permanent replacement (after obtaining CBB approval), within 120 calendar days of the vacancy occurring. Pending the appointment of a permanent replacement, the licensee must make immediate interim arrangements to ensure continuity of the duties and responsibilities of the controlled function affected, provided that such arrangements do not pose a conflict of duties. These interim arrangements must be approved by the CBB.**

CRA-1.7.10 The notification should identify if the planned move was prompted by any concerns over the person concerned, or is due to a routine staff change, retirement or similar reason.

CRA-1.7.10A **Licensees must immediately notify the CBB in case of any material change to the information provided in a Form 3 submitted for an approved person.**

Amendment of Authorisation

CRA-1.7.10B **Licensees must seek prior CBB approval before an approved person may move from one controlled function to another within the same licensee.**

CRA-1.7.10C For the purposes of Paragraph CRA-1.7.10B, a new application should be completed and submitted to the CBB. A person may be considered 'fit and proper' for one controlled function, but not for another, if for instance the new role requires a different set of skills and experience.

CRA-1.7 Approved Persons (continued)

Cancellation of Approved Person Status

CRA-1.7.11 The CBB may also move to declare someone as not 'fit and proper', in response to significant compliance failures or other improper behaviour by that person.

CRA-1.7.12 [This Paragraph was deleted in xx 2023].

CRA-1.7.13 [This Paragraph was deleted in xx 2023].

CRA-1.7.14 **[This Paragraph was deleted in xx 2023].**

CRA-1.7.15 **[This Paragraph was deleted in xx 2023].**

CRA-1.7.16 [This Paragraph was deleted in xx 2023].

CRA-1.7.17 [This Paragraph was deleted in xx 2023].

CRA-1.7.18 **Where a firm is in doubt as to whether a function should be considered a controlled function it must discuss the case with the CBB.**

CRA-1.7.19 **Licensees must designate an employee, of appropriate standing and resident in Bahrain, as compliance officer. The duties of the compliance officer include:**

(a) Having responsibility for oversight of the licensee's compliance with the requirements of the CBB; and

(b) Reporting to the licensee's Board in respect of that responsibility.

MODULE	CRA:	Crypto-asset
CHAPTER	CRA-2	Licensing Condition

CRA-2.1 Condition 1: Legal Status

CRA-2.1.1 **The legal status of a licensed crypto-asset service licensee must be:**

(a) For undertaking Category-1, Category-2 and Category-3 regulated crypto-asset services

(i) A Bahraini company with limited liability ("W.L.L."); or

(ii) A Bahraini joint stock company (B.S.C.); or

(iii) [This Subparagraph was deleted in XX 2023].

(b) For undertaking Category-4 regulated crypto-asset services (Licensed crypto-asset exchange)

(i) A Bahraini joint stock company (B.S.C.); or

(ii) [This Subparagraph was deleted in XX 2023].

CRA-2.1.2 [This Paragraph was deleted in XX 2023].

CRA-2.2 Condition 2: Mind and Management

CRA-2.2.1 Licensees must have designated place of business within the Kingdom of Bahrain. Licensees with their Registered Office in the Kingdom of Bahrain must maintain their Head Office in the Kingdom.

CRA-2.2.2 The CBB requires the following approved persons occupying controlled functions must be resident in Bahrain:

(a) Chief Executive Officer or General Manager;
(b) Compliance Officer;
(c) Money Laundering Reporting Officer;
(d) Head of Finance;
(e) Head of Risk Management;
(f) Head of Operations; and
(g) Chief Information Security Officer.

CRA-2.2.3 [This Paragraph was deleted in XX 2023].

CRA-2.3 Condition 3: Substantial Shareholders

CRA-2.3.1 **Licensees must satisfy the CBB that their substantial shareholders are suitable and pose no undue risks to the licensee.**

CRA-2.3.2 For the purposes of this Module "substantial shareholder" means a person who alone or together with his associates:

(a) Holds not less than 5% of the shares in the licensee; or

(b) Is in a position to control not less than 5% of the votes in the licensee.

CRA-2.4 Condition 4: Board and Employees

CRA-2.4.1 **As per Article 65(a) of the CBB law, those nominated to carry out controlled functions must satisfy CBB's approved person's requirements.**

CRA-2.4.2 The definition of controlled functions as well as the CBB's approved person requirements are contained in Section CRA-1.7.

CRA-2.4.3 **The licensee's staff must collectively provide a sufficient range of skills and experience to manage the affairs of the licensee in a sound and prudent manner. Licensees must ensure their employees meet any training and competency requirements specified by the CBB.**

CRA-2.5 Condition 5: Financial Resources

CRA-2.5.1 **Licensees must maintain a level of financial resources, as agreed with the CBB, adequate for the level of business proposed. The level of financial resources held must always equal or exceed the minimum requirements contained in Chapter CRA-3.**

CRA-2.5.2 **[This Paragraph was deleted in XX 2023].**

CRA-2.5.3 The CBB, in its complete discretion may ask for a guarantee from the potential licensee's (applicant's) controlling or major shareholders or the ultimate beneficiaries on a case by case basis as it deems appropriate/necessary as part of the required documents to be submitted as mentioned in Paragraph CRA-1.2.4.

CRA-2.6 Condition 6: Systems and Controls

CRA-2.6.1 Licensees must maintain systems and controls that are adequate for the scale and complexity of their activities. These systems and controls, at a minimum, must meet the requirements contained in Chapter CRA-5 (Technology Governance and Cyber Security), Chapter CRA-6 (Risk Management) and the requirements of Module HC (High-level Controls) of the CBB Rulebook Volume 6.

CRA-2.6.2 Licensees must maintain adequate segregation of responsibilities in their staffing arrangements, to protect against the misuse of systems or errors. Such segregation must ensure that no single individual has control over all stages of a transaction.

CRA-2.6.3 Licensees must maintain systems and controls that are adequate to address the risks of financial crime occurring in the licensee. These systems and controls must meet the minimum requirements contained in Module AML of the CBB Rulebook Volume 6.

CRA-2.6.4 [This Paragraph was deleted in XX 2023].

CRA-2.6.5 Licensees must, in connection with any client assets received in the course of their business, establish and maintain separate client accounts, segregated from those used for their own funds, as specified in Section CRA-4.5.

CRA-2.6.6 [This Paragraph was deleted in XX 2023].

CRA-2.6.7 [This Paragraph was deleted in XX 2023].

CRA-2.7 Condition 7: External Auditor

CRA-2.7.1 Pursuant to Article 61 of the CBB Law, Licensees must appoint external auditors, subject to prior CBB approval. Licensees must comply with the minimum requirements regarding auditors contained in Section CRA-4.2.

CRA-2.7.2 Applicants must submit details of their proposed external auditor to the CBB as part of their license application.

CRA-2.8 Condition 8: Other Requirements

Books and Records

CRA-2.8.1 **Licensees must maintain comprehensive books of accounts and other records, which must be available for inspection within the Kingdom of Bahrain by the CBB, or persons appointed by the CBB, at any time. Licensees must ensure that all relevant books and other information, as may be required by the CBB, are kept for a minimum period of 10 years.**

General Conduct

CRA-2.8.2 **Licensees must conduct their activities in a professional and orderly manner, in keeping with good market practice standards. Licensees must comply with the general standards of business conduct as well as the standards relating to treatment of clients contained in Chapter CRA-4 and CRA-12.**

Additional Conditions

CRA-2.8.3 **Licensees must comply with any other specific requirements or restrictions imposed by the CBB on the scope of their license.**

CRA-2.8.4 In addition, the CBB may vary existing requirements or impose additional restrictions or requirements, beyond those already specified for licensees, to address specific risks.

CRA-3.1 General Requirements

Obligation to Maintain Adequate Capital

CRA-3.1.1 **Licensees are required to ensure that the minimum capital is paid into a retail bank licensed to operate in the Kingdom of Bahrain. They must provide, upon request, evidence to the CBB of the deposited amount.**

CRA-3.1.2 **The minimum capital requirement comprising of paid-up share capital, unimpaired by losses, for respective category of licensees are indicated in the table below:**

Minimum Capital Requirement

Sl. No.	Licensing Category	Minimum Capital (BD)
1.	Category-1	25,000
2.	Category-2	100,000
3.	Category-3	200,000
4.	Category-4	300,000

CRA-3.1.3 **In addition to the minimum capital requirements specified in CRA-3.1 onwards, the CBB may, at its discretion, require licensees to hold additional capital in an amount and form as the CBB determines, should this be necessary (in the CBB's view) to ensure the financial integrity of the licensee and its ongoing operations.**

CRA-3.1.4 For the purposes of determining the additional amount of capital that must be maintained by a licensee, the CBB may consider a variety of factors, including but not limited to:

(a) The composition of the licensee's total assets, including the position, size, liquidity, risk exposure, and price volatility of each type of crypto asset;
(b) The composition of the licensee's total liabilities, including the size and repayment timing of each type of liability;
(c) The actual and expected volume of the licensee's crypto asset business activity;
(d) The liquidity position of the licensee;
(e) The types of products or services to be offered by the licensee;
(f) There is a change in the business of the licensee that the CBB considers material;

CRA-3.1 General Requirements (continued)

(g) The licensee is exposed to risk or elements of risks that are not covered or not sufficiently covered by the minimum capital requirement;
(h) The prudential valuation of the trading book is insufficient to enable the licensee to sell or hedge out its position within a short period without incurring material losses under normal market conditions; and
(i) The licensee fails to establish or maintain an adequate level of additional capital to ensure that (i) cyclical economic fluctuations do not lead to a breach of the minimum capital requirement; or (ii) the capital requirement can absorb the potential losses and risks.

CR-3.1.5 **In the event that a licensee fails to meet any of the requirements specified in this Section, it must, on becoming aware that it has breached the minimum capital requirements, immediately notify the CBB in writing. Unless otherwise directed, the licensee must in addition submit to the CBB, within 30 calendar days of its notification, a plan demonstrating how it will achieve compliance with these requirements.**

CRA-3.2 Key Requirements

CRA-3.2.1 Licensees dealing in crypto assets as principal and thereby taking proprietary positions in crypto assets must ensure that their proprietary positions (at cost) do not exceed 50% of the paid-up capital or net shareholders' equity, whichever is lower.

CRA-3.2.2 [This Paragraph was deleted in XX 2023].

CRA-3.2.3 Pursuant to Article 57(a) of the CBB Law, a licensee must seek CBB approval before making any modification to its issued or paid-up capital. In the case that a licensee has been granted approval to increase its paid-up capital, confirmation from its external auditor stating that the amount has been deposited in the licensee's bank account will subsequently be required.

CRA-3.3 Additional Requirements

CRA-3.3.1 **A licensee's liquid assets must be held in a form acceptable to the CBB, in a minimum amount of three months estimated expenditures including salaries, rent, general utilities and other operating costs.**

CRA-3.3.2 Liquid assets comprise of cash, cash equivalents, and placements or deposits maturing within 30 days.

CRA-4.1 General Obligations

CRA-4.1.1 In the course of undertaking regulated crypto-asset services, a licensee must:

(a) Ensure that the regulated activities are undertaken in a fair, orderly and transparent manner;

(b) Manage any risks associated with its business and operations prudently;

(c) Not act contrary to the interests of its clients and its investors;

(d) Maintain proper arrangements to enforce compliance with the CBB Law, Rules and Regulations and develop, implement and adhere to a "crypto-asset compliance policy", tailored to meet specific crypto-asset services requirements. The crypto asset compliance policy must reflect a clear comprehension and understanding of compliance responsibilities with respect to crypto-assets;

(e) Act with due skill, care and diligence in all dealings with clients;

(f) Identify clients' specific requirements in relation to the services about which they are enquiring;

(g) Provide sufficient information to enable clients to make informed decisions when purchasing services offered to them;

(h) Provide sufficient and timely documentation to clients to confirm that their transaction arrangements are in place and provide all necessary information about their rights and responsibilities;

(i) Maintain fair treatment of clients through the lifetime of the client relationships, and ensure that clients are kept informed of important events and are not mislead;

(j) Ensure complaints from clients are dealt with fairly and promptly;

(k) Take appropriate measures to safeguard any money and crypto-assets handled on behalf of clients and maintain confidentiality of client information;

(l) Use or arrange to use a well-designed Business Continuity Plan and Disaster Recovery Plan;

(m) Ensure that all its employees or representatives are provided with the required education, qualifications and experience and they fully understand the Rules and regulations of the CBB;

(n) Ensure that there are sufficient and appropriate records, books and systems in place to record all transactions and maintain an audit trail;

CRA-4.1 General Obligations (continued)

(o) Have an operating manual and internal policies;

(p) Provide to the CBB, for its review and comment, the draft agenda at least 5 business days prior to, the shareholders' meetings (i.e. ordinary and extraordinary general assembly);

(q) Ensure that any agenda items to be discussed or presented during the course of meetings which requires the CBB's prior approval, have received the necessary approval, prior to the meeting taking place;

(r) Invite a representative of the CBB to attend any shareholders' meeting that will take place. The invitation must be provided to the CBB at least 5 business days prior to the meeting taking place; and

(s) Within one month of any shareholders' meetings referred to in Paragraph CRA-4.1.1(p), provide to the CBB a copy of the minutes of the meeting.

(t) [This Subparagraph was deleted in XX 2023].

CRA-4.1.1A Licensees must ensure that all regulated financial services are provided without any discrimination based on gender, nationality, origin, language, faith, religion, physical ability or social standing.

CRA-4.1.2 A licensee must establish and document keyman risk management measures that include arrangements in place should individuals holding encryption keys or passcodes to stored assets, including wallets, or information be unavailable unexpectedly due to death, disability or other unforeseen circumstances.

CRA-4.1.3 A licensee must ensure that it maintains no encrypted accounts that cannot be retrieved in the future for any reason. It must also advise its clients who maintain wallets with firms outside Bahrain (i.e. not CBB licensees) and not licensed by the CBB about any associated risks.

CRA-4.1 General Obligations (continued)

CRA-4.1.4 **Licensees must use appropriate technology and wherever appropriate third-party services to identify the situations referred to below, and other additional mitigating or preventive actions as necessary to mitigate the money laundering and terror financing risks involved. The situations include amongst others:**

(a) The use of proxies, any unverifiable or high-risk IP geographical locations, disposable email addresses or mobile numbers, or frequently changing the devices used to conduct transactions; and

(b) Transactions involving tainted wallet addresses such as "darknet" marketplace transactions and those involving tumblers.

CRA-4.1.5 **Licensees must establish and maintain adequate and effective systems and processes, including suspicious transaction indicators to monitor transactions with a client or counterparty involving crypto- assets and conduct appropriate enquiry and evaluation of potentially suspicious transactions identified. In particular:**

(a) Identify transactions with wallet addresses or their equivalent which are compromised or tainted; and

(b) Employ technology solutions which enable the tracking of crypto-assets through multiple transactions to more accurately identify the source and destination of these crypto- assets.

CRA-4.1.6 For the purposes of CRA-4.1.5(a), a wallet address is compromised or tainted where there is reasonable suspicion that it is used for the purpose of conducting fraud, identity theft, extorting ransom or any other criminal activity.

Suitability and Appropriateness Assessment for Retail Clients

CRA-4.1.7 **Licensees, prior to offering portfolio management service, investment advice or complex products such as but not limited to derivative products, margin or leverage products or products with features that may make it difficult for a retail investor to understand the essential characteristics of the product and its risks (including the pay-out structure and how the product may perform in different market and economic conditions), must undertake a suitability and appropriateness assessment for retail clients (investors other than accredited investors) to determine the suitability and appropriateness of crypto-assets products and services for retail clients. Licensees must gather sufficient information from every retail client to be in a position to decide whether the crypto-asset product and/or services are suitable and appropriate for the client.**

CRA-4.1 General Obligations (continued)

CRA-4.1.8 Licensees may seek the following information for the purposes of suitability and appropriateness assessment:

(a) Client's knowledge and experience:
  (i) the types of investment services and transaction which the client is familiar with;
  (ii) the nature, volume and frequency of the client's transactions with trading and investments; and
  (iii) the level of education, profession or (if relevant) former profession of the client.

(b) Client's financial situation:
  (i) the source and extent of the client's regular income;
  (ii) the client's assets, including liquid assets, investments and real property;
  (iii) the client's regular financial commitments;
  (iv) the ability to bear losses.

(c) Client's investment objective:
  (i) the client's investment horizon;
  (ii) the client's risk preferences, risk profile and risk tolerance; and
  (iii) the purposes of the investment.

Transaction with Unknown Counterparties

CRA-4.1.9 A licensee should take reasonable measures to avoid transactions with another crypto-asset entity, infrastructure or service provider where the counterparty is unknown or anonymous (e.g., via certain peer to peer or decentralised exchanges) at any stage of its business process.

CRA-4.2 Auditors and Accounting Standards

CRA-4.2.1 **Licensees must appoint external auditor for its accounts for every financial year. While appointing an auditor, licensees must exercise due skill, care and diligence in the selection and appointment of the auditor and must take into consideration the auditor's experience and track record of auditing crypto-asset related businesses.**

CRA-4.2.1A In accordance with Article 61(b) of the CBB Law, if a licensee fails to appoint an auditor within four months from the beginning of the financial year, the CBB shall appoint such auditor.

CRA-4.2.1B **The licensee must pay the fees of the auditor regardless of the manner in which such auditor is appointed.**

CRA-4.2.1C **An auditor must not be the chairman or a director in the licensee's board or a managing director, agent, representative or taking up any administrative work therein, or supervising its accounts, or a next of kin to someone who is responsible for the administration or accounts of a licensee, or having an extraordinary interest in a licensee.**

CRA-4.2.1D **If any of the circumstances referred to in rule CRA-4.2.1C occurs after the appointment of the auditor, the licensee must appoint another external auditor.**

CRA-4.2.1E **Licensees must provide the external auditor with all information and assistance necessary for carrying out his duties.**

CRA-4.2.1F **The duties of the external auditor must include the preparation of a report on the final accounts. The report must contain a statement on whether the licensee's accounts are correct and reflect the actual state of affairs of the licensee according to the auditing standards prescribed by the CBB, and whether the licensee has provided the auditor with all required information and clarifications.**

CRA-4.2.1G **The final audited accounts must be presented to the general meeting of the licensee together with the auditor's report. A copy of these documents must be sent to the CBB at least 15 days before the date of the general meeting.**

CRA-4.2.2 **Audited financial statements of a licensee must be prepared in accordance with the International Financial Accounting Standards (IFRS) or AAOIFI standards as appropriate.**

CRA-4.2 Auditors and Accounting Standards (continued)

Annual Audited Financial statements

CRA-4.2.3 Licensees must submit to the CBB their annual audited financial statements no later than 3 months from the end of the licensee's financial year. The financial statements must include the statement of financial position (balance sheet), the statements of income, cash flow and changes in equity and where applicable, the statement of comprehensive income.

Annual Report

CRA-4.2.5 Licensees must submit a soft copy (electronic) of their full annual report to the CBB within 4 months of the end of their financial year.

Reviewed (Unaudited) Quarterly Financial Statements

CRA-4.2.6 Licensees must submit to the CBB unaudited quarterly financial statements (in the same format as their Annual Audited Accounts), reviewed by the licensee's external auditor, on a quarterly basis within 45 calendar days from the end of each of the first 3 quarters of their financial year.

CRA-4.3 Listing of Crypto-assets

CRA-4.3.1 This section outlines the frameworks, criteria and obligations for listing of crypto-assets by a licensee.

CRA-4.3.2 **[This Paragraph was deleted in XX 2023].**

CRA-4.3.2A **Licensees are allowed to undertake spot trading (spot market) in crypto-assets.**

CRA-4.3.2B The CBB may, at its sole discretion, allow a licensee to list and conduct trading activities in derivatives of crypto-assets such as, but not limited to, futures, options, indices, contract for difference (CFD's), swaps etc provided the CBB is satisfied that the licensee has a comprehensive derivative transactions risk management framework. The aforementioned risk management framework should provide appropriate measure to mitigate, amongst others, market risk, credit risk, liquidity risk, settlement risk, operational risk and legal risk. In addition, the derivative transaction risk management framework should also include guidelines for stress testing, back testing, settlement process, margin methodology, derivative product selection policy, client exposure limit and suitability and appropriateness policy.

CRA-4.3.3 [This Paragraph was deleted in XX 2023].

CRA-4.3.4 **[This Paragraph was deleted in XX 2023].**

CRA-4.3.5 [This Paragraph was deleted in XX 2023].

Crypto-asset Listing Policy

CRA-4.3.6 **Licensees must establish and adopt a board approved crypto-asset listing policy in accordance with the framework stipulated in this Section.**

CRA-4.3.7 **Licensees must, prior to commencement of business operations, provide a copy of the crypto-asset listing policy to the CBB. Unless the CBB raises specific concerns with respect to the board approved crypto-asset listing policy, licensees may implement the policy and self-certify crypto-assets for listing on its platform.**

CRA-4.3 Listing of Crypto-assets (continued)

CRA-4.3.8 **Prior to listing a crypto-asset, a licensee must notify the CBB of its intent to list the crypto-asset, provide the findings of the risk assessment undertaken in accordance with Paragraph CRA- 4.3.14 along with the board resolution approving the crypto-asset. The licensee must confirm in its notification to CBB that the proposed new crypto-asset complies with the requirements of its crypto-asset listing policy.**

CRA-4.3.9 **Licensees must provide a list of all the crypto-assets listed on its platform no later than 10 days from the end of each quarter.**

CRA-4.3.10 **The crypto-asset listing policy referred to in Paragraph CRA-4.3.6 must include robust procedures that comprehensively address all steps involved in the review and approval of crypto-assets. Licensees must have necessary monitoring capability (e.g. via monitoring systems, internal monitoring control, on-chain analysis etc.) in place before listing of the crypto-asset on its platform.**

CRA-4.3.11 The crypto-asset listing policy should help establish a mechanism for approval of a crypto-asset only if the licensee unambiguously concludes that the listing and trading of the crypto-asset is consistent with the CBB's approach to establish a fair, transparent and orderly crypto-asset market, complies with applicable laws, rules and regulations and is not detrimental to the interest of the market or client.

CRA-4.3.12 **Licensees must not list crypto-assets that facilitate or may facilitate the obfuscation or concealment of the identity of a client or counterparty or crypto-assets that are designed to, or substantially used to circumvent laws and regulations. Licensees must ensure that they only list crypto-assets to which they have in place the necessary AML monitoring capabilities.**

CRA-4.3 Listing of Crypto-assets (continued)

CRA-4.3.13 Licensees must ensure that:

(a) Decisions to approve or disapprove each new crypto-asset is taken in accordance with the crypto-asset listing policy;

(b) Any actual or potential conflicts of interest in connection with the review and decision-making process have been assessed and effectively addressed, whether such actual or potential conflicts of interest are related to the licensee's board members, shareholders employees, their families, or any other party;

(c) Records are readily available for the CBB's review, of the crypto-asset listing policy's application to each crypto-asset. This includes the final approval for listing of a crypto-asset, the documents reviewed including an assessment of all associated material risks in connection with each crypto-asset approval or disapproval, such as reviews and sign-offs by various departments of the licensee, such as the legal, compliance, cybersecurity, and operations department etc.;

(d) The crypto-asset listing policy is reviewed annually to ensure that it continues to properly identify, assess, and mitigate the relevant risks and to ensure the robustness of the governance, monitoring and oversight framework;

(e) It informs the CBB immediately, at any time after the submission of its crypto-asset listing policy to CBB, if the said policy ceases to comply with the general framework laid out in this Section; and

(f) It does not make any changes or revisions to its crypto-asset listing policy without the prior written approval of its Board. A copy of the revised crypto-asset listing policy along with the written Board approval must be submitted to the CBB.

Risk Assessment

CRA-4.3.14 Licensees must establish criteria and undertake a comprehensive risk assessment of the crypto-assets that it intends to list on its platform. The assessment must include, but are not limited to, the following:

(a) Licensees must conduct a thorough due diligence process to ensure that the crypto-asset is created or issued for lawful and legitimate purposes, and not for evading compliance with applicable laws and regulations (e.g., by facilitating money laundering or other illegal activities) and that the process is subject to a strong governance and control framework.

(b) Licensees must consider the following factors while undertaking the due diligence:

CRA-4.3 Listing of Crypto-assets (continued)

(i) The technological experience, track record and reputation of the issuer and its development team;
(ii) The availability of a reliable multi-signature hardware wallet solution;
(iii) The protocol and the underlying infrastructure, including whether it is: (1) a separate blockchain with a new architecture system and network or it leverages an existing blockchain for synergies and network effects, (2) scalable, (3) new and/or innovative or (4) the crypto-asset has an innovative use or application;
(iv) The relevant consensus protocol;
(v) Developments in markets in which the issuer operates;
(vi) The geographic distribution of the crypto-asset and the relevant trading pairs, if any;
(vii) Whether the crypto-asset has any in-built anonymization functions; and
(viii) Crypto-asset exchanges on which the crypto-asset is traded.

(c) Operational risks associated with a crypto-asset. This includes the resulting demands on the licensee's resources, infrastructure, and personnel, as well as its operational capacity for continued client on-boarding and client support based on reasonable forecasts considering the overall operations of the licensee;
(d) Risks associated with any technology or systems enhancements or modification requirements necessary to ensure timely adoption or listing of any new crypto-asset;
(e) Risks related to cybersecurity: Whether the crypto-asset is and will be able to withstand, adapt and respond to cyber security vulnerabilities, including size, testing, maturity, and ability to allow the appropriate safeguarding of secure private keys;
(f) Traceability/Monitoring of the crypto-asset: Whether licensees are able to demonstrate the origin and destination of the specific crypto-asset, whether the crypto-asset enables the identification of counterparties to each trade, and whether transactions in the crypto-asset can be adequately monitored;
(g) Market risks, including minimum market capitalisation, price volatility, concentration of crypto-asset holdings or control by a small number of individuals or entities, price manipulation, and fraud;

CRA-4.3 Listing of Crypto-assets (continued)

(h) Risks relating to code defects and breaches and other threats concerning a crypto-asset and its supporting blockchain, or the practices and protocols that apply to them;
(i) Risks relating to potential non-compliance with the requirements of the licensee's condition and regulatory obligations as a result of the listing of new crypto-asset;
(j) Legal risks associated with the new crypto-asset, including any pending or potential civil, regulatory, criminal, or enforcement action relating to the issuance, distribution, or use of the new crypto-asset; and
(k) 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 and whether this is a new distributed ledger that has been demonstrably stress tested.

Periodic Monitoring

CRA-4.3.15 Licensees must have policies and procedures in place to monitor the listed crypto-assets to ensure that continued use of the crypto-asset remains prudent. This includes:
(a) Periodic re-evaluation of crypto-assets, including whether material changes have occurred, with a frequency and level of scrutiny tailored to the risk level of individual crypto-assets, provided that the frequency of re-evaluation must at a minimum be annual;
(b) Implementation of control measures to manage risks associated with individual crypto-assets; and
(c) The existence of a process for de-listing of crypto-assets, including notice to affected clients and counterparties in the case of such de-listing.

CRA-4.3 Listing of Crypto-assets (continued)

Disclosure

CRA-4.3.16 Licensees must make disclosures, which are easily accessible and prominently visible to clients, for each listed crypto-asset, containing at a minimum, the following information:

(a) Details about the crypto-asset: the type of crypto-asset (payment token, asset token, utility token, stablecoin etc.), its function and details about the asset(s) where a crypto-asset is backed by asset(s);

(b) The risks related to the specific crypto-asset such as, but not limited to, price volatility and cyber-security; and

(c) Any other information that would assist clients to make an informed investment decision.

CRA-4.3.17 Licensees must prominently display on their platform the following statement, "THE CENTRAL BANK OF BAHRAIN HAS NEITHER REVIEWED NOR APPROVED THE LISTED CRYPTO-ASSETS".

CRA-4.3.18 Where the CBB determines that undertaking regulated services in a crypto-asset may be detrimental to the financial sector of the Kingdom of Bahrain and/or it may affect the legitimate interest of clients, the licensees, based on the instruction of the CBB, must delist the crypto-asset. In such scenarios, the licensee shall remain responsible for orderly settlement of trade and any liability arising due to the delisting of the crypto-asset.

CRA-4.4 Dealing with Clients

CRA-4.4.1 Licensees must not undertake transactions with a person(s) unless they have been registered as a client(s) in accordance with the requirements of this Module.

CRA-4.4.2 Licensees must ensure their compliance with the applicable laws and regulations in the jurisdictions to which they provide regulated crypto-asset services.

CRA-4.4.3 Licensees must not register an applicant as a client where the applicant and/or the beneficial owner(s) or the ultimate beneficial owner is/are domiciled in Non-Cooperative Countries or Territories ('NCCTS'). Paragraph AML-9.1.1(a) and (b) of Module AML provides the basis for identification of the Non-Cooperative Countries or Territories.

CRA-4.4.4 Licensees must, at the time of registration, verify and obtain a signed statement from applicants confirming whether or not the applicant is acting on their own.

CRA-4.4.5 Prior to commencement of business transactions, licensees must:
(a) Seek and register bank accounts details and other types of accounts details to be used for receipt or transfer of fiat funds (such as credit cards and pre-paid cards) of the clients; and
(b) Verify the bank accounts and other types of accounts details provided by a client to ensure that the bank accounts and other accounts are in the name of the registered client.

CRA-4.4.6 The bank accounts and other accounts details provided by the client must be used for the purpose of transfer of fiat funds between the client and the licensee. A licensee must not deposit and/or withdraw fiat funds through any account other than those accounts which are in the name of the client and registered with the licensee for the said purpose.

CRA-4.4 Dealing with Clients (continued)

CRA-4.4.7 Where an applicant's IP address is masked, a licensee must take reasonable steps to unmask the IP address or decline to provide services to that applicant.

CRA-4.4.8 Licensees must not allow a single client to open multiple accounts.

CRA-4.4.9 At the time of registration, licensees must set a trading limit, position limit or both with reference to the client's financial situation with a view to ensuring that the client has sufficient financial capability to be able to assume the risks and bear the potential trading losses. The limit applicable to a client must be reviewed by the licensee on a periodic basis and in light of any material change in the client's financial situation.

CRA-4.5 Client Protection

Segregation and Handling of Clients' Assets

CRA-4.5.1 **Licensees undertaking regulated crypto-asset service and authorised to hold clients' assets must apply the same standards and comply with the requirements of segregation and handling of clients' assets Rules set out in this Section.**

CRA-4.5.1A For the purpose of this Module, "clients assets" means crypto-assets, money and other assets received or held on behalf of a client by the licensee and any crypto-assets, money or other assets accruing therefrom.

CRA-4.5.2 **For purposes of safeguarding client's rights in relation to crypto-assets and client money which are held or controlled by the licensee, a licensee must hold clients' money and/or to crypto-assets in specially created and segregated accounts. These accounts must be identified separately from any other accounts used to hold money and/or to crypto-assets belonging to the licensee.**

CRA-4.5.3 **A licensee must obtain a written declaration from the entities with whom the licensee has deposited client assets that the said entity renounces and will not attempt to enforce or execute, any charge, right of set-off or other claim against the account.**

Client Money

CRA-4.5.4 **A licensee must properly handle and safeguard client money. The arrangement to handle and safeguard client money, must include, but not be limited to the following:**

(a) Establishing one or more client bank accounts with a retail bank licensed in the Kingdom of Bahrain for safekeeping of client money;

(b) Client money must not be paid out of a client bank account other than for:

(i) Paying the client on whose behalf it is being held;

(ii) Meeting the client's settlement obligations in respect of dealings in crypto-assets carried out by the licensee for the client, being the client on whose behalf it is being held;

(iii) Paying money that the client owes to the licensee in respect of the conduct of regulated crypto-asset services; or

(iv) Paying in accordance with the client's written instructions, including standing authorities or one-off directions.

CRA-4.5 Client Protection (continued)

(c) Not used for licensee's own use or given as collateral for any purpose to a third party or be subject to any restrictions; and
(d) Reported as a separate balance sheet item in the licensee's financial statements specifying also the nature and purpose for which such funds are held on behalf of its customers.

CRA-4.5.5 Client money must be received by the licensee directly into a client bank account.

CRA-4.5.5A A licensee must match any unidentified receipts in its client bank accounts with all relevant information in order to establish the nature of any payment and the identity of the person who has made it. Where the receipt is not client money, within one business day of becoming so aware, that amount of money should be paid out of the client bank account.

Reconciliation of Clients' Money

CRA-4.5.6 Licensees must reconcile, at least on a monthly basis, the balance on each client's money account as recorded by the licensee with the balance on that account as set out in the statement issued by the entity with whom the licensee has deposited client money.

CRA-4.5.7 Licensees must also reconcile, at least on a monthly basis, the total of the balances on all client money accounts as recorded by the licensee with the total of the corresponding credit balances in respect of each of its clients as recorded by the licensee.

CRA-4.5.7A Licensees must ensure that the client money reconciliations referred to in Paragraphs CRA-4.5.6 and CRA-4.5.7 are completed within 10 business days from the end of the months. Any differences, shortfalls and excess balances must be investigated, and corrective measures taken to restore correct client asset balance.

CRA-4.5 Client Protection (continued)

Risk Disclosure to Clients

CRA-4.5.8 As part of establishing a relationship with a client, and prior to entering into an initial transaction with such client, licensee must disclose in clear, conspicuous, and legible writing in both Arabic and English languages, all material risks associated with crypto-asset products and services including at a minimum, the following:

(a) A crypto-asset is not a legal tender and is not backed by the government;

(b) legislative and regulatory changes or actions at national level or international level may adversely affect the use, transfer, exchange, and value of crypto-assets;

(c) transactions in crypto-assets may be irreversible, and, accordingly, losses due to fraudulent or accidental transactions may not be recoverable;

(d) some crypto-asset transactions may be deemed to be made when recorded on a public ledger, which is not necessarily the date or time that the client initiates the transaction;

(e) the value of crypto-assets may be derived from the continued willingness of market participants to exchange fiat currency for crypto-asset, which may result in the potential for permanent and total loss of value of a particular crypto-asset should the market for that crypto-asset disappear;

(f) the volatility and unpredictability of the price of crypto-assets relative to fiat currency may result in significant loss over a short period of time;

(g) [This Subparagraph was deleted in XX 2023];

(h) the nature of crypto-assets means that any technological difficulties experienced by the licensee may prevent the access or use of a client's crypto-assets; and

(i) any investor protection mechanism.

CRA-4.5 Client Protection (continued)

Disclosure of General Terms and Conditions

CRA-4.5.9 When registering a new client, and prior to entering into transactions with such client, a licensee must disclose in clear, conspicuous, and legible writing in both Arabic and English languages, all relevant terms and conditions associated with its products and services including at a minimum, the following:

(a) the client's liability for unauthorized crypto-asset transactions;
(b) the client's right to stop payment of a preauthorized crypto-asset transfer and the procedure to initiate such a stop-payment order;
(c) under what circumstances the licensee will disclose information concerning the client's account to third parties;
(d) the client's right to receive periodic account statements from the licensee;
(e) the client's right to receive a confirmation note or other evidence of a transaction;
(f) the client's right to prior notice of a change in the licensee's rules or policies or terms and conditions; and
(g) [This Subparagraph was deleted in XX 2023].
(h) cybersecurity risks associated with crypto-assets including the risk of partial or full loss of crypto-assets in the event of a cyber-attack, and measures that have been put in place to mitigate the cyber security risks.

CRA-4.5.9A In addition to the disclosure requirements stipulated in Paragraph CRA-4.5.9, Category-1, Category-2 and Category-3 crypto-asset licensees must disclose, in writing, the following information to clients:

(a) How they execute and route client's order and source liquidity (e.g. whether they pass or route orders to an exchange to execute). Where the licensee routes client orders to one or more crypto-asset exchanges for execution, it must disclose details of all the crypto-asset exchanges;
(b) Whether it may carry trading in crypto-assets as principal, and if so, whether, it may trade against client's position; and
(c) How it determines the prices of the crypto-assets it quotes to clients.

CRA-4.5 Client Protection (continued)

Disclosure of the Terms of Transactions

CRA-4.5.10 Prior to each transaction in a crypto-asset with a client, a licensee must furnish to the client a written disclosure in clear, conspicuous, and legible writing in both Arabic or English languages, containing the terms and conditions of the transaction, which must include, at a minimum, to the extent applicable:

(a) the amount of the transaction;
(b) any fees, expenses, and charges borne by the client, including applicable exchange rates;
(c) the type and nature of the crypto-asset transaction;
(d) a warning that once executed the transaction may not be undone; and
(e) such other disclosures as are customarily given in connection with a transaction of this nature.

Acknowledgement of Disclosure

CRA-4.5.11 A licensee must ensure that all disclosures required in this Section are acknowledged as received by clients.

Confirmation Note

CRA-4.5.12 Upon completion of any transaction, a licensee must provide to the client a confirmation note containing the following information:

(a) the type, value, date, and precise time of the transaction;
(b) the fee charged;
(c) the exchange rate, if applicable;
(d) the name and contact information of the licensee, including a telephone number established by the licensee to answer questions and register complaints;

CRA-4.5.12A Where a client undertakes more than one transaction, the licensee may prepare a single confirmation note which:

(a) Records all of those transactions; and
(b) In respect of each of those transactions includes all of the information which would have been required to be included in the confirmation note.

CRA-4.5.12B Licensees must provide the confirmation note to the client no later than the end of the business day on which the transaction was undertaken.

CRA-4.5 Client Protection (continued)

CRA-4.5.13 [This Paragraph was deleted in XX 2023].

Prevention of Fraud

CRA-4.5.14 Licensees must take reasonable steps to detect and prevent fraud, including by establishing and maintaining a written anti-fraud policy. The anti-fraud policy must, at a minimum, include:

(a) the identification and assessment of fraud-related risk areas;
(b) procedures and controls to protect against identified risks;
(c) allocation of responsibility for monitoring risks and establish real-time/near real-time fraud risk monitoring and surveillance system; and
(d) procedures for the periodic evaluation and revision of the anti-fraud procedures, controls, and monitoring mechanisms.

CRA-4.5.14A A client account must be considered dormant if the client does not trade for a period of 12 (twelve) continuous months. All the accounts designated as dormant need to be monitored carefully in order to avoid unauthorized transactions in the account.

CRA-4.5.14B If a client wishes to make his/her account active after 12 continuous months or thereafter, the licensee must ensure that the client submits a request to reactivate his/her account. In case there is any change in the information such as; address, contact details, email ID, bank account, financial disclosure provided in KYC at the time of registration as client, the same must be submitted along with the request. After verification of the updated / revised details and approval from the compliance officer or money laundering reporting officer (MLRO), the account can be made active and transactions can take place.

Client Agreements and Statements

CRA-4.5.15 Licensees must not provide a regulated crypto-asset service to a client as mentioned unless there is a client agreement entered into between the licensee and the client containing the key information specified in Rule CRA-4.5.16.

CRA-4.5 Client Protection (continued)

CRA-4.5.16 The client agreement referred to in Rule CRA-4.5.15 must include:

(a) The name and address of the licensee;
(b) The regulatory status of the licensee;
(c) When and how the client agreement is to come into force and how the agreement may be amended or terminated;
(d) Details of fees, costs and other charges and the basis upon which the licensee will impose those fees, costs and other charges;
(e) Sufficient details of the service that the licensee will provide, including where relevant, information about any product or other restrictions applying to the licensee in the provision of its services and how such restrictions impact on the service offered by the licensee; or if there are no such restrictions, a statement to that effect;
(f) Details of any conflicts of interests;
(g) Any soft dollar arrangements;
(h) Key particulars of the licensee's complaints handling procedures or dispute resolution procedure; and
(i) The crypto-asset risk disclosure referred to in Rule CRA-4.5.8 and disclosure of general terms and conditions referred to in Rule CRA-4.5.9.

CRA-4.5.16A Licensees must provide periodic statements i.e. confirmation note, monthly statement of account and annual statement of account to their clients. Licensees may provide to their clients the periodic statement information through their website and/or application. Where a licensee provides the periodic statement through its website and application, the licensee is not required to send the periodic statement to their clients separately.

Monthly Statement of Account

CRA-4.5.17 A licensee must prepare and provide a monthly statement of account to the client no later than 7 business days following the month where any of the following circumstances apply:

(a) During a month, the licensee has provided a confirmation note (refer CRA-4.5.12) or has received funds from the client;
(b) At any time during a month, the client has an account balance (funds) that is not nil; or
(c) At any time during a month, crypto-assets are held for the account of the client.

CRA-4.5 Client Protection (continued)

CRA-4.5.18 The monthly statement of account referred to in Paragraph CRA-4.5.17 must include the following information:

(a) The name and address of the licensee;
(b) The name, address and account number of the client;
(c) The date on which the statement of account is issued;
(d) The outstanding balance of that account as at the beginning and as at the end of the month;
(e) Details of all transactions undertaken by the client during the month;
(f) Inward and outward transfer of crypto-assets during the month;
(g) The quantity, and, in so far as readily ascertainable, the market price and total value of each crypto-asset held at the end of the month;
(h) Details of all funds credited to and fees and charges levied during the month; and
(i) Details of any restrictions, such as blocks pursuant to an order by a court or other competent authority.

Duty to Provide Statement of Account on Request

CRA-4.5.19 Where a licensee receives a request from a client for a statement of account it must provide the client, as soon as practicable after the date of the request but no later than 5 working days from the date of the request, such statement of account which must include the information required as per Paragraph CRA-4.5.18 for the period specified by the client.

CRA-4.5.20 Where a licensee provides the statement of account at the request of the client (refer to CRA-4.5.19), it may impose a reasonable charge on the client for providing the statement of account.

CRA-4.5.21 A licensee must prepare and provide a statement of account to the client, on an annual basis, no later than the end of the seventh business day after the end of the financial year except under following circumstances:

(a) There are no transactions;
(b) The account balance (funds) is nil; and
(c) The balance of crypto-assets held on behalf of the client is nil.

No Restriction on Withdrawal of Client Assets

CRA-4.5.22 Where a client requests for withdrawal of client assets, a licensee, unless the restriction is pursuant to a freeze or block order from a court or due to factors related to money laundering and terror financing (suspicious transactions), must not impose restriction on withdrawal of the client assets held under its control.

CRA-4.6 Marketing and Promotion

CRA-4.6.1 In all advertising and marketing materials, licensees and any person or entity acting on its behalf, must not, directly or by implication, make any false, misleading, or deceptive representations or omissions.

CRA-4.6.1A Licensees must ensure that all advertising and marketing materials adhere to the principles of fair competition. While comparative advertisement in product or service promotion is acceptable, the intent and connotation of comparative advertisement should be to inform and never to discredit or unfairly target competitors, competing products or services.

CRA-4.6.2 Licensees must not advertise its products, services, or activities in the Kingdom of Bahrain without including the name of the licensee and a statement that the licensee is "Licensed by the CBB as a crypto-asset service provider (Licensing category-…)".

CRA-4.6.3 Licensees must not make use of the name of the CBB in any promotion in such a way that would indicate endorsement or approval of its products or services.

CRA-4.6.4 [This Paragraph was deleted in XX 2023].

CRA-4.6.5 Licensees, at a minimum, must make the following information available on its website:

(a) The services being offered;
(b) Its trading and operational rules as well as admission and removal rules and criteria;
(c) Its admission and trading fees and charges, including illustrative examples of how the fees and charges are calculated, for ease of understanding by clients;
(d) The relevant material information for each crypto-asset, including providing clients with access to up-to-date whitepaper or information, and providing clients with material information as soon as reasonably practicable to enable clients to appraise the position of their investments (for example, any major events in relation to a crypto-asset or any other material information);
(e) The rights and obligations of the licensee and the client;
(f) Arrangements for dealing with settlement failures in respect of transactions executed on its platform;

CRA-4.6 Marketing and Promotion (continued)

(g) Detailed documentation of market models, order types as well as deposit and withdrawal processes for fiat currencies and crypto-assets;
(h) Where applicable, client's liability for unauthorised crypto asset transactions;
(i) Client's right to stop transfer of a preauthorised crypto-asset and the procedure for initiating such a stop-transfer order;
(j) Circumstances under which the licensee may disclose the client's confidential information to third parties, including regulators;
(k) Client's right to prior notice of any change in the licensee's rules, policies and terms and conditions;
(l) Dispute resolution mechanisms, including complaints procedures; and
(m) System upgrades and maintenance procedures and schedules.

Licensees must, as soon as practicable thereafter, publish any revisions or updates on its website and circulate them to the users of its platforms, identifying the amendments which have been made and providing an explanation for making them.

Promotion

CRA-4.6.6 Licensees must ensure that all the following requirements are met with regards to promotion of products or services:
(a) They do not involve a breach of Bahrain law or any other relevant applicable law, rules or regulation;
(b) All documentation concerning promotions is in a language that clients can fully understand;
(c) Clients to whom promotions are directed must have equal opportunity in terms of access and treatment;
(d) The communication concerning promotions must be clear, concise, truthful, unambiguous and complete to enable clients to make a fully informed decision;
(e) Where the promotion involves communication of earnings potential or benefits associated with the products or services promoted, all costs, charges or levies and risks are also disclosed; and
(f) Licensees using social media platforms as a medium of promotion must provide a reference or link to more comprehensive information available elsewhere.

CRA-4.7 Complaints

CRA-4.7.1 Licensees must establish and maintain written policies and procedures to resolve complaints in a fair and timely manner.

CRA-4.7.2 A licensee must provide, in a clear and conspicuous manner on their website and in all physical locations the following disclosures:

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

(b) [This Subparagraph was deleted in XX 2023];

(c) The CBB's mailing address, website, and telephone number.

CRA-4.7.3 Licensees must notify to the CBB any change in their complaint policies or procedures within seven days prior to the implementation of the new complaint policy.

CRA-4.7.4 The complaint handling procedures of a licensee must provide for:

(a) The receipt of written complaints;

(b) The appropriate investigation of complaints;

(c) An appropriate decision-making process in relation to the response to a customer complaint;

(d) Notification of the decision to the customer;

(e) The recording of complaints; and

(f) How to deal with complaints when a business continuity plan (BCP) is operative.

CRA-4.7.5 A licensee's internal complaint handling procedures must be designed to ensure that:

(a) All complaints are handled fairly, effectively and promptly;

(b) [This Subparagraph was deleted in XX 2023];

(c) The number of unresolved complaints referred to the CBB is minimized;

(d) The employee responsible for the resolution of complaints has the necessary authority to resolve complaints or has ready access to an employee who has the necessary authority;

(e) Relevant employees are aware of the licensee's internal complaint handling procedures that they comply with them and receive training periodically to be kept abreast of changes in procedures; and

(f) Complaints are investigated by an employee of sufficient competence who, where appropriate, was not directly involved in the matter which is the subject of a complaint.

CRA-4.7 Complaints (Continued)

Response of Complaints

CRA-4.7.6 Licensees must acknowledge in writing customer written complaints within 5 working days of receipt.

CRA-4.7.7 Licensees must respond to a client complaint promptly and within a period of 4 weeks of receiving the complaint or provide the complainant with an appropriate explanation as to why the licensee is not, at that time, in a position to respond and must indicate by when the licensee will respond.

Redress

CRA-4.7.8 Licensees must decide and communicate how it proposes to provide the customer with redress. Where appropriate, the licensee must explain the options open to the customer and the procedures necessary to obtain the redress.

CRA-4.7.9 Where a licensee decides that redress in the form of compensation is appropriate, the licensee must provide the complainant with fair compensation and must comply with any offer of compensation made by it which the complainant accepts.

CRA-4.7.10 Where a licensee decides that redress in a form other than compensation is appropriate, it must provide the redress as soon as practicable.

CRA-4.7.11 A licensee must inform the clients who have filed a complaint with the licensee and are not satisfied with the response received as per Paragraph CRA-4.7.7, about their right to forward the complaint to the Consumer Protection Unit at the CBB within 30 calendar days from the date of receiving the letter from the licensee.

CRA-4.7 Complaints (Continued)

Reporting of Complaints

CRA-4.7.12 Licensees must submit to the Consumer Protection Unit at the CBB, a quarterly report summarising the following:

(a) The number of complaints received during the quarter;
(b) The substance of the complaints;
(c) The number of days it took the licensee to acknowledge and to respond to the complaints; and
(d) The status of the complaint, including whether resolved or not, and whether redress was provided.

CRA-4.7.13 Where no complaints have been received by the licensee within the quarter, a 'nil' report must be submitted to the Consumer Protection Unit at the CBB.

Record of Complaints

CRA-4.7.14 A licensee must maintain a record of all client complaints. The record of each complaint must include:

(a) The identity of the complainant;
(b) The substance of the complaint;
(c) The status of the complaint, including whether resolved or not, and whether redress was provided; and
(d) All correspondence in relation to the complaint.

Such records must be retained by the licensee for a period of 10 years from the date of receipt of the complaint.

CRA-4.8 Professional Indemnity Coverage

Key Provisions

CRA-4.8.1 Licensees handling client asset and/or client money must maintain a professional indemnity coverage (insurance policy) in accordance with the scope of coverage provided in Paragraph CRA-4.8.3.

CRA-4.8.2 For the purposes of Paragraph CRA-4.8.1, licensees must maintain professional indemnity coverage for an amount that is determined based on its assessment of the potential risk exposure. Such amount, however, must not be less than BD100,000.

CRA-4.8.3 Licensees must ensure that the Professional Indemnity Coverage, *inter alia*:

(a) Covers any legal liability in consequence of any negligent act, error or omission in the conduct of the licensee's business by the licensee or any person employed by it or otherwise acting for it, including consultants under a contract for service with the licensee;

(b) Covers legal defence costs which may arise in consequence of any negligent act, error or omission in the conduct of the licensee's business by the licensee or any person employed by it or otherwise acting for it, including consultants under a contract for service with the licensee;

(c) Covers any legal liability in consequence of any dishonest, fraudulent, criminal or malicious act, error or omission of any person at any time employed by the licensee, or otherwise acting for it, including consultants under a contract for service with the licensee; and

(d) Covers loss of and damage to documents and records belonging to the licensee or which are in the care, custody or control of the licensee or for which the licensee is responsible; including also liability and costs and expenses incurred in replacing, restoring or reconstructing the documents or records; including also consequential loss resulting from the loss or damage to the documents or records.

CRA-4.8 Professional Indemnity Coverage (continued)

CRA-4.8.4 **The professional indemnity coverage must be obtained from an insurance firm acceptable to the CBB and licensed in the Kingdom of Bahrain. Licensees must submit a Professional Indemnity Insurance Return (Form PIIR) on an annual basis. Additionally, they must provide, upon request, evidence to the CBB of the coverage in force.**

CRA-4.8.5 **[This Paragraph was deleted in XX 2023].**

CRA-4.8.6 The requirement to maintain professional indemnity coverage will normally be met by the licensee obtaining an insurance policy from an insurance firm. The CBB may also accept an insurance indemnity policy issued at group level, e.g. issued with respect to the parent of the licensee, provided the terms of the policy explicitly provide indemnity coverage with respect to the licensee and meets the requirements of Paragraphs CRA-4.8.1, CRA-4.8.2 and CRA-4.8.3.

CRA-4.8.7 Upon written application to the CBB, the requirement in Rule CRA-4.8.1 may instead be met by the licensee depositing with a retail bank licensed to operate in the Kingdom of Bahrain, an amount, specified by the CBB, to be held in escrow against future claims. This amount will not be less than the minimum required policy limit.

CRA-4.8.8 **The policy must contain a clause that it may not be cancelled or lapsed without the prior notification of the CBB. The policy must also contain a provision for an automatic extended reporting period in the event that the policy is cancelled or lapsed, such that claims relating to the period during which the policy was in force may subsequently still be reported.**

CRA-4.9 Other Obligations

Obligation to Maintain Proper Records

CRA-4.9.1 **[This Paragraph was deleted in XX 2023].**

Obligation to Maintain Confidentiality

CRA-4.9.2 **A licensee must maintain the confidentiality of all client information in accordance with the requirements of the Personal Data Protection Law (PDPL).**

Records of Telephone conversations and Electronic Communications

CRA-4.9.3 **[This Paragraph was deleted in XX 2023].**

CRA-4.10 Matters Requiring Approval of CBB

CRA-4.10.1 **A licensee must comply with the following Rules of relating to a change of shareholding held by substantial shareholders, or a transfer of business or substantially all its assets or liabilities in the same manner set out in:**

(a) Section MIR-5 (Substantial Shareholding in a Licensed Member);
(b) Section MIR-6 (Control of a Licensed Member); and
(c) Section MIR-7 (Business Transfer).

Dividends

CRA-4.10.2 **Licensees must obtain the CBB's prior written approval to any dividend proposed to be distributed to the shareholders, before announcing the proposed dividend by way of press announcement or any other means of communication and prior to submitting a proposal for a distribution of profits to a shareholder vote.**

CRA-4.10.3 One of the factors that the CBB will consider while determining whether to grant an approval is when it is satisfied that the level of dividend proposed is unlikely to leave the licensee vulnerable to breaching the CBB's financial resources requirements, taking into account, as appropriate, the trends in the licensee's business volumes, profitability, expenses and performance.

CRA-4.10.4 **To facilitate the prior approval required under Paragraph CRA-4.10.2, licensees must provide the CBB with:**

(a) The licensee's intended percentage and amount of proposed dividends for the coming year;
(b) A letter of no objection from the licensee's external auditor on such profit distribution; and
(c) A detailed analysis of the impact of the proposed dividend on the capital adequacy requirements outlined in Chapter CRA-3 (Minimum Capital Requirements) and the liquidity position of the licensee.

CRA-4.11 Compliance

CRA-4.11.1 **Licensees must establish, implement and maintain adequate policies and procedures designed to detect any risk of failure by the licensee to comply with its obligations under the CBB Law, its regulations, resolutions and directives (including these Rules), as well as to detect the associated risks, and must put in place adequate measures and procedures designed to minimize such risk and to enable the CBB to exercise its powers effectively.**

CRA-4.11.2 For the purposes of Paragraph CRA-4.11.1, licensees should take into account the nature, scale and complexity of its business and the nature and range of regulated crypto-asset services undertaken in the course of the business.

CRA-4.11.3 **Licensees must establish and maintain a permanent and effective compliance function which operates independently and has, as a minimum, the following responsibilities:**

(a) To monitor and, on a regular basis, to assess the adequacy and effectiveness of the measures and procedures put in place, and the actions taken to address any deficiencies in the licensee's compliance with its obligations;

(b) To draw up and implement a compliance monitoring plan; and

(c) To advise and assist the relevant persons responsible for carrying out regulated crypto-asset services to comply with the licensee's legal and regulatory obligations.

CRA-4.11.4 **In order to enable the compliance function to discharge its responsibilities properly, licensees must ensure that the following conditions, as a minimum, are satisfied:**

(a) The compliance function must have the necessary authority, resources, expertise and access to all relevant information;

(b) A Compliance Officer must be appointed and shall be responsible for the compliance function and for any reporting as to compliance required by these Rules;

(c) The relevant persons involved in the compliance function must not be involved in the performance of services or activities which they monitor; and

(d) The method of determining the remuneration of the relevant persons involved in the compliance function must not compromise their objectivity.

CRA-4.11 Compliance (Continued)

CRA-4.11.5 The CBB may exempt a licensee from the requirements Paragraph CRA-4.11.4(c) if the licensee is able to demonstrate to the satisfaction of the CBB, that in view of the nature, scale and complexity of its business, and the nature and range of regulated crypto-asset services and related activities, the requirement under Paragraph CRA-4.11.4(c) is not proportionate and that its compliance function continues to be independent, objective and effective.

CRA-4.11.6 The CBB may, at its discretion, allow the compliance officer of a licensee to also act as the licensee's Money Laundering Reporting Officer, provided the licensee is able to demonstrate to the satisfaction of the CBB, that the nature, scale and complexity of the business is such that both the functions can be carried out effectively by the compliance officer without compromising on supervisory objectives.

CRA-4.12 Additional requirements applicable to Crypto-asset Exchange Licensees

CRA-4.12.1 **[This Paragraph was deleted in XX 2023].**

CRA-4.12.2 **[This Paragraph was deleted in XX 2023].**

CRA-4.12.3 **[This Paragraph was deleted in XX 2023].**

Suspension of trading and delisting

CRA-4.12.4 **Where a licensed crypto-asset exchange decides to delist or suspend the trading of one or more crypto-assets, it must notify the CBB with the rationale for the suspension or delisting of the crypto-asset.**

CRA-4.12.5 **Without prejudice to the right of the CBB to demand suspension or delisting of a crypto-asset from trading, a licensed crypto-asset exchange must suspend or delist from trading a crypto-asset which no longer complies with the Rules of the licensed crypto-asset exchange unless such suspension or delisting would likely cause significant damage to the clients' interests or the orderly functioning of the market.**

CRA-4.12.6 **Where a licensed crypto-asset exchange decides to suspends or delists from trading a crypto-asset, it must by way of a public announcement inform the clients' regarding the date of suspension or delisting of the crypto-asset.**

CRA-4.12.7 Where a llicensed crypto-asset exchange has suspended or delisted a crypto-asset from trading, the CBB may require that other licensees, which fall under its jurisdiction and trade the same crypto-asset, also suspend or delist that crypto-asset from trading, where the suspension or delisting is due to suspected market abuse, a take-over bid or the non-disclosure of inside information about the issuer or crypto-asset except where such suspension or delisting could cause significant damage to the clients' interests or the orderly functioning of the market.

CRA-4.12 Additional Requirements Applicable to Crypto-asset Exchange Licensees (Continued)

Order Matching

CRA-4.12.8 A licensed crypto-asset exchange must ensure expedient and accurate verification of trades and matching settlement instructions.

CRA-4.12.9 A licensed crypto-asset exchange must ensure that it has necessary systems and controls to verify the existence of funds and crypto-assets, as applicable, of clients submitting orders.

Pre-trade transparency

CRA-4.12.10 A licensed crypto-asset exchange must disclose to its clients and the public as appropriate, on a continuous basis during normal trading, the following information relating to trading of crypto-assets on its platform:

(a) The current bid and offer prices and volume;
(b) The depth of trading interest shown at the prices and volumes advertised through its systems for the crypto-assets; and
(c) Any other information relating to crypto-assets which would promote transparency relating to trading.

CRA-4.12.11 A licensed crypto-asset exchange must use appropriate mechanisms to enable pre-trade information to be made available to the public in an easy to access and uninterrupted manner.

Post-trade transparency

CRA-4.12.12 A licensed crypto-asset exchange must disclose the price, volume and time of the transactions executed in respect of crypto-assets to the public as close to real-time as is technically possible on a non-discretionary basis. A licensed crypto-asset exchange must use adequate mechanisms to enable post-trade information to be made available to the public in an easy to access and uninterrupted manner, at least during business hours.

Client Record Keeping

CRA-4.12.13 A licensed crypto-asset exchange must keep, for at least 10 years, the relevant data relating to all orders and all transactions in crypto-assets which are carried out through their systems.

CRA-4.12 Additional Requirements Applicable to Crypto-asset Exchange Licensees (Continued)

CRA-4.12.14 For the purposes of Paragraph CRA-4.12.10, the records must contain the relevant data that constitute the characteristics of the order, including those that link an order with the executed transaction(s) that stems from that order. This shall include:

(a) Details of the names and numbers of the crypto- assets bought or sold;
(b) The quantity;
(c) The dates and times of execution;
(d) The transaction prices; and
(e) A designation to identify the clients in relation to which that transaction has been executed;

CRA-4.12.15 A licensed crypto-asset exchange must maintain adequate resources and have back-up facilities in place in order to be capable of reporting at all times.

CRA-4.12.16 [This Paragraph was deleted in XX 2023].

CRA-4.12.17 [This Paragraph was deleted in XX 2023].

Exchange Systems

CRA-4.12.18 A licensed crypto-asset exchange must have in place effective systems, procedures and arrangements to reject orders that exceed pre-determined volume and price thresholds or are clearly erroneous.

CRA-4.12 Additional Requirements Applicable to Crypto-asset Exchange Licensees (Continued)

CRA-4.12.19 A licensed crypto-asset exchange must be able to temporarily halt or constrain trading if there is a significant price movement in a crypto-asset on its platform or a related platform during a short period and, in exceptional cases, to be able to cancel, vary or correct any transaction.

CRA-4.12.20 A licensed crypto-asset exchange must report the reasons for halting trading and any material changes to those reasons to the CBB in a consistent and comparable manner.

CRA-4.12.21 A licensed crypto-asset exchange must ensure that its fee structures are transparent, fair and non-discriminatory and that they do not create incentives to place, modify or cancel orders or to execute transactions in a way which contributes to disorderly trading conditions or market abuse.

CRA-4.12.22 A licensed crypto-asset exchange must ensure that its rules on co-location services are transparent, fair and non-discriminatory.

CRA-4.12.23 A licensed crypto-asset exchange must be able to identify, by means of flagging from its clients, orders generated by algorithmic trading, the different algorithms used for the creation of orders and the relevant persons initiating those orders.

CRA-4.12.24 A licensed crypto-asset exchange must, upon request by the CBB, make available to the CBB, data relating to the order book or give the CBB access to the order book so that it is able to monitor trading.

Settlement

CRA-4.12.25 A licensed crypto-asset exchange must establish procedures that enable the confirmation of relevant details of transactions in crypto-assets.

CRA-4.12.26 A licensed crypto-asset exchange's settlement procedures must clearly define the point at which settlement is final.

CRA-4.12.27 A licensed crypto-asset exchange must complete final settlement no later than the end of the trade date, and preferably intraday or in real time, to reduce settlement risk.

CRA-4.12 Additional Requirements Applicable to Crypto-asset Exchange Licensees (Continued)

CRA-4.12.28 A licensed crypto-asset exchange must clearly define the point after which unsettled payments, transfer instructions, or other obligations may not be revoked by a client.

CRA-4.12.29 A licensed crypto-asset exchange must minimize and strictly control the credit and liquidity risk arising from money settlements.

CRA-4.12.30 A licensed crypto-asset exchange must clearly state its obligations with respect to the delivery of crypto-assets and should identify, monitor, and manage the risks associated with such delivery.

CRA-4.12.31 A licensed crypto-asset exchange must have in place adequate systems to safeguard against settlement failures as well as resolution systems which cater for such failures. Such systems should be clearly documented in the licensed crypto-asset exchange's policies, procedures and rules.

CRA-4.12.32 A licensed crypto-asset exchange must establish a system that monitors settlement failures of transactions in crypto-assets. Upon occurrence of such events, the licensed crypto-asset exchange must immediately report to the CBB, details of the settlement failure and any other relevant information.

Rules of a Licensed Crypto-asset Exchange

CRA-4.12.33 A licensed crypto-asset exchange must issue clear and transparent Rules in order to ensure that any crypto-assets being traded on its platform is being traded in a fair, orderly and efficient manner. Such rules, and any changes or amendments thereto are to be approved by the CBB.

CRA-4.12.34 The CBB may require a licensed crypto-asset exchange to effect any changes to its rules, as it may deem necessary.

CRA-4.12 Additional Requirements Applicable to Crypto-asset Exchange Licensees (Continued)

CRA-4.12.35 The rules must, *inter alia*, include Sections on:

(a) The administration of the licensed crypto-asset exchange, including but not limited to governance, compliance and risk management;

(b) How the licensed crypto-asset exchange operates, including the client on boarding procedure, the procedure for the listing of crypto-assets, trading procedures, pre- and post-trade transparency, market monitoring, custody and safekeeping arrangements, record keeping, and fees;

(c) The reporting of suspicious transactions;

(d) Settlement and resolution mechanisms in the event of settlement failure;

(e) Suspension and removal from trading;

(f) Business continuity; and

(g) Actions or measures which the licensed crypto-asset exchange can take against its clients.

Inability to Discharge Functions

CRA-4.12.36 Where, due to the occurrence of any event or circumstances, a licensed crypto-asset exchange is unable to discharge any of its functions whatsoever, it must on the day of such occurrence immediately notify the CBB of its inability to discharge that function, specifying:

(a) The event or circumstance causing it to become unable to discharge any of its functions;

(b) The functions which the licensed crypto-asset exchange is unable to discharge; and

(c) What action, if any, is being taken or is being proposed by the licensed crypto-asset exchange in order to deal with the situation and, in particular, to be able to recommence discharging that function.

CRA-4.12 Additional Requirements Applicable to Crypto-asset Exchange Licensees (continued)

Actions or Measures

CRA-4.12.37 Where a licensed crypto-asset exchange has taken any action against any of its clients, including the suspension of the client from trading, the blacklisting or expelling of a client or any other action, in respect of a breach of its rules, that licensed crypto-asset exchange must immediately notify the CBB of that event, providing:

(a) The name of the person concerned;
(b) Brief description of the breach;
(c) Details of the action or measure taken by the licensed crypto-asset exchange; and
(d) The reasons for taking that action or measure.

CRA-5.1 General Requirements

CRA-5.1.1 Licensees must have in place clear and comprehensive policies and procedures, from a technology perspective, for the following key areas:

(a) 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).

CRA-5.1.2 Licensees must, as a minimum, have in place systems and controls with respect to the following:

(a) Crypto-asset Wallets: Procedures describing the creation, management and controls of crypto-asset wallets, including:

(i) Wallet setup/configuration/deployment/deletion/backup and recovery;

(ii) Wallet access privilege management;

(iii) Wallet user management;

(iv) Wallet Rules and limit determination, review and update; and

(v) Wallet audit and oversight.

(b) Private keys: Procedures describing the creation, management and controls of private keys, including:

(i) Private key generation;

(ii) Private key exchange;

(iii) Private key storage;

(iv) Private key backup;

(v) Private key destruction; and

(vi) Private key access management.

CRA-5.1 General Requirements (continued)

(c) Origin and destination of crypto-assets: Systems and controls to mitigate the risk of misuse of crypto-assets, setting out how:

(vii) The origin of crypto-asset is determined, in case of an incoming transaction; and

(viii) The destination of crypto-asset is determined, in case of an outgoing transaction.

(d) Security: A security plan describing the security arrangements relating to:

(i) The privacy of sensitive data;

(ii) Networks and systems;

(iii) Cloud based services;

(iv) Physical facilities; and

(v) Documents, and document storage.

(e) Risk management: A risk management plan containing a detailed analysis of likely risks with both high and low impact, as well as mitigation strategies. The risk management plan must cover, but is not limited to:

(i) Operational risks;

(ii) Technology risks, including 'hacking' related risks;

(iii) Market risk for each crypto-asset; and

(iv) Risk of financial crime.

CRA-5.1.3 The CBB may grant exemptions from specific requirements of technology governance and cyber security. A licensee seeking exemption from specific requirements must provide in writing, to the satisfaction of the CBB, that the nature, scale and complexity of their business does not require such technology governance and cyber security measures and in absence of such measures there will be no risk of violation of applicable laws, including the CBB Law, its regulations, resolutions or directives (including these rules) or risks associated with the integrity of the market and/or interest of clients.

System Resilience

CRA-5.1.4 **Licensees must have in place effective systems, procedures and arrangements to ensure that their IT systems including the trading and settlement systems, are resilient, have sufficient capacity to deal with peak order and message volumes, are able to ensure orderly trading under conditions of severe market stress, are fully tested to ensure such conditions are met and are subject to effective business continuity arrangements to ensure continuity of their services if there is any failure of their trading systems.**

CRA-5.1 General Requirements (continued)

CRA-5.1.5 Licensees must continuously monitor the utilisation of their system resources against a set of pre-defined thresholds. Such monitoring must facilitate the licensee in carrying out capacity management to ensure IT resources are adequate to meet current and future business needs.

CRA-5.1.6 Licensees must conduct regular testing of resilience of its IT systems to meet its business requirements.

CRA-5.1.7 A licensee's IT systems must be designed and implemented in a manner to achieve the level of system availability that is commensurate with its business needs. Fault-tolerant solutions must be implemented for IT systems which require high system availability and technical glitches must be minimized.

CRA-5.2 Maintenance and Development of Systems

CRA-5.2.1 Licensees must have a clear and well-structured approach for the implementation and upgrade of systems and software.

CRA-5.2.2 Licensees must 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). Licensees must ensure that the implementation of new systems, or upgrading of existing systems, is thoroughly checked by multiple members of technology staff.

CRA-5.2.3 Licensees must ensure that any changes made to a codebase in use are tracked and recorded, with a clear audit trail for appropriate internal checks and sign-offs.

CRA-5.2.4 For the purposes of Rule CRA-5.2.3, the use of version control software which allows for the accurate timestamping and identification of the user responsible for relevant changes must be considered.

CRA-5.2.5 Licensees must maintain a clear and comprehensive audit trail for system issues internally, including security issues and those with third parties, and their resolution.

CRA-5.2.6 [This Paragraph was deleted in January 2020].

CRA-5.2.7 [This Paragraph was deleted in XX 2023].

CRA-5.2.8 [This Paragraph was deleted in XX 2023].

CRA-5.2.9 [This Paragraph was deleted in XX 2023].

CRA-5.3 Security Measures and Procedures

CRA-5.3.1 Licensees must 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, must be performed as soon as safely feasible after such updates and patches have been released.

CRA-5.3.2 The IT infrastructures must provide strong layered security and ensure elimination of "single points of failure". Licensees must maintain IT infrastructure security policies, describing in particular how strong layered security is provided and how "single points of failure" are eliminated. IT infrastructures must be strong enough to resist, without significant loss to clients, 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.

CRA-5.3.3 Licensees must regularly test security systems and processes. System components, processes, and custom software must be tested frequently to ensure security controls continue to reflect a changing environment.

CRA-5.3.4 Licensees must have in place policies and procedures that address information security for all staff sets the security tone for the whole entity and informs staff what is expected of them. All staff should be aware of the sensitivity of data and their responsibilities for protecting it.

CRA-5.3.5 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.

CRA-5.3.6 Licensees must conduct regular security tests of their systems, network, and connections.

CRA-5.4 Cryptographic Keys and Wallet Storage

CRA-5.4.1 **Licensees must implement robust procedures and protective measures to ensure the secure generation, storage, backup and destruction of both public and private keys.**

CRA-5.4.2 In order to access crypto assets, the device on which the private key is held needs access to a network (which, in most cases is through 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.

CRA-5.4.3 **Crypto-assets that do not need to be immediately available must be held offline, in a 'cold wallet' (refer to CRA-8.1.9).**

Password protection and encryption

CRA-5.4.4 **Both hot and cold wallets must be password protected and encrypted. The key storage file that is held on the online or offline device must be encrypted. The user is therefore protected against theft of the file (to the degree the password cannot be cracked). However, malware on the machine may still be able to gain access (e.g., a keystroke logger to capture the password).**

CRA-5.4.5 **Licensees must use multi-signature wallets (e.g., where multiple private keys are associated with a given public key and a subset of these private keys, 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 offer more security because a user can still gain access to its crypto-assets when two or more Private Keys remain available. (see also CRA-4.1.2 and CRA-4.1.3).**

Off Line Storage of Keys

CRA-5.4.6 To mitigate the risks associated with hot wallets, private keys can be stored in a cold wallet, which is not attached to a network. Licensees should implement cold wallet key storage where possible if they are offering wallet services to their Clients.

CRA-5.4 Cryptographic Keys and Wallet Storage (continued)

Air Gapped Key Storage

CRA-5.4.7 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 should 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 Deliver Key

CRA-5.4.8 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.

CRA-5.4.9 **Licensees offering deterministic wallet solutions must ensure that users are provided with clear instructions for situations where keys, seeds or hardware supporting such wallet solutions are lost.**

Private Key Management

CRA-5.4.10 **A licensee must establish and implement strong internal controls and governance procedures for private key management to ensure all cryptographic seeds and private keys are securely generated, stored and backed up. A licensee using a third party crypto-asset custodian must ensure that the third-party custodian establishes and implements such controls and procedures. The procedure must include the following:**

(a) The generated seed and private key must be sufficiently resistant to speculation or collusion. The seed and private key should be generated in accordance with applicable international security standards and industry best practices, so as to ensure that the seeds (where Hierarchical Deterministic Wallets, or similar processes, are used) or private keys (if seed is not used) are generated in a non-deterministic manner that ensures randomness so that they are not reproducible. Where practicable, seed and private key should be generated offline and kept in a secure environment, such as a Hardware Security Module (HSM), with appropriate certification for the lifetime of the seeds or private keys;

CRA-5.4 Cryptographic Keys and Wallet Storage (continued)

(b) Detailed specifications for how access to cryptographic devices or applications is to be authorised, covering key generation, distribution, use and storage, as well as the immediate revocation of a signatory's access as required;

(c) Access to seed and private key relating to crypto-assets is tightly restricted among approved persons, no single approved person has possession of information on the entirety of the seed, private key or backup passphrases, and controls are implemented to mitigate the risk of collusion among authorised personnel; and

(d) Distributed backups of seed or private key is kept so as to mitigate any single point of failure. The backups need to be distributed in a manner such that an event affecting the primary location of the seed or private key does not affect the backups. The backups should be stored in a protected form on external media (preferably HSM with appropriate certification). Distributed backups should be stored in a manner that ensures seed and private key cannot be re-generated based solely on the backups stored in the same physical location. Access control to the backups must be as stringent as access control to the original seed and private key.

Private Key Storage Policy

CRA-5.4.11 Licensees must establish, maintain and implement a private key storage policy to ensure effective and prudent safekeeping of the seed and private key at all times. In particular, such policy must address:

(a) The keyman risk associated with the storage of seed and private key is appropriately addressed;

(b) The seed and private key can be retrieved at a short notice without excessive reliance on one or more individuals who may be unavailable due to death, disability or other unforeseen circumstances; and

(c) Where a licensee maintains a physical copy of the seed and private key, the physical copies of seed and private key must be maintained in Bahrain in a secure and indestructible manner and the same can be used to access the wallets if a need arises.

The private key storage policy along with other documents and evidences confirming that the seed and private key are held securely must be made available to the CBB upon request.

CRA-5.5 Origin and Destination of Crypto-asset

CRA-5.5.1 Licensees must consider using technology solutions and other systems to adequately meet anti-money laundering, financial crime and know-your-customer requirements.

CRA-5.5.2 Licensees must develop, implement and maintain effective transaction monitoring systems to determine the origin of a crypto-asset, to monitor its destination and to apply strong "know your transaction" measures which enable the licensees to have complete granular data centric information about the transactions conducted by a client.

CRA-5.5.3 Licensees must be vigilant and establish internal processes and indicators to identify crypto-assets that may have been tainted i.e. used for an illegal purpose (for example, certain client or use of "mixer" and "tumbler" services).

CRA-5.6 Planned and Unplanned System Outages

CRA-5.6.1 **Licensees must have multiple communication channels to ensure that its clients are informed, ahead of time, of any outages which may affect them.**

CRA-5.6.2 **Licensees must have clear, publicly available, procedures articulating the process in the event of an unplanned outage. During an unplanned outage, licensees must be able to rapidly disseminate key information and updates on a frequent basis.**

CRA-5.6.3 Licensees should have a programme of planned systems outages to provide for adequate opportunities to perform updates and testing.

CRA-5.7 [This Section was deleted in XX 2023]

CRA-5.7.1 [This Paragraph was deleted in XX 2023].

CRA-5.7.2 [This Paragraph was deleted in XX 2023].

CRA-5.7.3 [This Paragraph was deleted in XX 2023].

CRA-5.8 Cyber Security

General Requirements

CRA-5.8.1 A licensee must establish and maintain an effective cyber security program to ensure the availability and functionality of the licensee's electronic systems and to protect those systems and any sensitive data stored on those systems from unauthorized access, use, or tampering. The cyber security program must be designed to perform, at the minimum, the following five core cyber security functions:

(a) identify internal and external cyber security risks by, at a minimum, identifying the information stored on the licensee's systems, the sensitivity of such information, and how and by whom such information may be accessed;
(b) protect the licensee's electronic systems, and the information stored on those systems, from unauthorized access, use, or other malicious acts through the use of defensive infrastructure and the implementation of policies and procedures;
(c) detect system intrusions, data breaches, unauthorized access to systems or information, malware, and other cyber security events;
(d) respond to detected cyber security events to mitigate any negative effects; and
(e) recover from cyber security events and restore normal operations and services.

CRA-5.8.1A Licensees must have a robust cyber security risk management framework that encompasses, at a minimum, the following components:

(a) Cyber security strategy;
(b) Cyber security policy; and
(c) Cyber security risk management approach, tools and methodology and, an organization-wide security awareness program.

CRA-5.8.1B The cyber security risk management framework must be developed in accordance with the National Institute of Standards and Technology (NIST) Cyber security framework which is summarized in Appendix A – Cyber security Control Guidelines. Broadly, the cyber security risk management framework should be consistent with the licensee's risk management framework.

CRA-5.8.1C Senior management, and where appropriate, the boards, should receive comprehensive reports, covering cyber security issues such as the following:

(a) Key Risk Indicators/ Key Performance Indicators;
(b) Status reports on overall cyber security control maturity levels;
(c) Status of staff Information Security awareness;

CRA-5.8 Cyber Security (continued)

(d) Updates on latest internal or relevant external cyber security incidents; and
(e) Results from penetration testing exercises.

CRA-5.8.1D Licensees may establish a cyber security committee that is headed by an independent senior manager from a control function (like CRO), with appropriate authority to approve policies and frameworks needed to implement the cyber security strategy, and act as a governance committee for the cyber security function. Membership of this committee should include senior management members from business functions, IT, Risk and Compliance.

Roles and Responsibilities of the Board

CRA-5.8.2 **The board must provide oversight and accord sufficient priority and resources to manage cyber security risk, as part of the licensee's overall risk management framework.**

CRA-5.8.3 **In discharging its oversight functions, the board must:**

(a) Ensure that the licensee's strategy, policy and risk management approach relating to cyber security are presented for the board's deliberation and approval;

(b) Ensure that the approved cyber security risk policies and procedures are implemented by the management;

(c) Monitor the effectiveness of the implementation of the licensee's cyber security risk policies and procedures and ensure that such policies and procedures are periodically reviewed, improved and updated, where required. This may include setting performance metrics or indicators, as appropriate, to assess the effectiveness of the implementation of cyber security risk policies and procedures;

(d) Ensure that adequate resources are allocated to manage cyber security including appointing a qualified person as Chief Information Security Officer ("CISO") with appropriate authority to implement the cyber security strategy. The CISO is the person responsible and accountable for the effective management of cyber security;

(e) [This Subparagraph was deleted in XX 2023];

(f) Ensure that the impact of cyber security risk is adequately assessed when undertaking new activities, including but not limited to any new products, investment decision, merger and acquisition, adoption of new technology and outsourcing arrangements; and

CRA-5.8 Cyber Security (continued)

(g) Ensure that adequate resources are allocated to manage cyber security including appointing a qualified person as Chief Information Security Officer ("CISO"). The CISO is the person responsible and accountable for the effective management of cyber security;
(h) Ensure that the management continues to promote awareness on cyber resilience at all levels within the entity;
(i) Ensure that the impact of cyber security risk is adequately assessed when undertaking new activities, including but not limited to any new products, investments decision, merger and acquisition, adoption of new technology and outsourcing arrangements; and
(j) Ensure that the board keeps itself updated and is aware of new or emerging trends of cyber security threats, and understand the potential impact of such threats to the licensee.

Roles and Responsibilities of the Management

CRA-5.8.4 The management is responsible for:
(a) Establishing and implementing cyber security policies and procedures that commensurate with the level of cyber security risk exposure and its impact on the licensee. These policies and procedures must take into account the following:
  (i) The sensitivity and confidentiality of data which the licensee maintains;
  (ii) Vulnerabilities of the licensee's information systems and operating environment across the licensee; and
  (iii) The existing and emerging cyber security threats.
(b) Ensuring that employees, agents (where relevant) and third party service providers are aware and understand the cyber security risk policies and procedures, the possible impact of various cyber security threats and their respective roles in managing such threats;
(c) Recommending to the board on appropriate strategies and measures to manage cyber security risk, including making necessary changes to existing policies and procedures, as appropriate; and
(d) Reporting to the board of any cyber security breaches and periodically update the board on emerging cyber security threats and their potential impact on the entity.

CRA-5.8 Cyber Security (continued)

CRA-5.8.4A **Management must ensure that:**

(a) The licensee has identified clear internal ownership and classification for all information assets and data;

(b) The licensee has maintained an inventory of the information assets and data which is reviewed and updated regularly;

(c) Employees responsible for cyber security are adequate to manage the licensee's cyber security risks and facilitate the performance and continuous improvement of all relevant cyber security controls; and

(d) It provides and requires employees involved in cyber security to attend regular cyber security update and training sessions (for example Security+, CEH, CISSP, CISA, CISM, CCSP) to stay abreast of changing cyber security threats and countermeasures.

CRA-5.8.4B With respect to Paragraph CRA-5.8.4A(a), data classification entails analyzing the data the licensee retains, determining its importance and value, and then assigning it to a category. When classifying data, the following aspects should be determined:

(a) Who has access to the data;
(b) How the data is secured;
(c) How long the data is retained (this includes backups);
(d) What method should be used to dispose of the data;
(e) Whether the data needs to be encrypted; and
(f) What use of the data is appropriate.

The general guideline for data classification is that the definition of the classification should be clear enough so that it is easy to determine how to classify the data. The owner of data (i.e. the relevant business function) should be involved in such classification.

Cyber Security Strategy

CRA-5.8.4C **An organisation-wide cyber security strategy must be defined and documented to include:**

(a) The position and importance of cyber security at the licensee;

(b) The primary cyber security threats and challenges facing the licensee;

(c) The licensee's approach to cyber security risk management;

(d) The key elements of the cyber security strategy including objectives, principles of operation and implementation approach;

(e) Scope of risk identification and assessment, which must include the dependencies on third party service providers;

(f) Approach to planning response and recovery activities; and

(g) Approach to communication with internal and external stakeholders, including sharing of information on identified threats and other intelligence among industry participants.

CRA-5.8 Cyber Security (continued)

CRA-5.8.4D The cyber security strategy should be communicated to the relevant stakeholders and it should be revised as necessary and, at least, once every three years. Appendix A provides cyber security control guidelines that can be used as a reference to support the licensee's cyber security strategy and cyber security policy.

Cyber Security Risk Policy

CRA-5.8.5 **Licensees must implement a written cyber security risk policy setting out the licensee's Board approved policies and related procedures that are approved by senior management, for the protection of its electronic systems and client data stored on those systems. This policy must be reviewed and approved by the licensee's board of directors at least annually. The cyber security policy, among others, must address the following areas:**

(a) A statement of the licensee's overall cyber risk tolerance as aligned with the licensee's business strategy. The cyber risk tolerance statement should be developed through consideration of the various impacts of cyber threats including customer impact, service downtime, recovery time objectives and occurrence/severity of cyber security breaches. The statement must also consider the impact on clients, potential negative media publicity, potential regulatory penalties, financial loss etc.;

(b) Strategy and measures to manage cyber security risk encompassing prevention, detection and recovery from a cyber security breach;

(c) Roles, responsibilities and lines of accountabilities of the board, the board committees, person responsible and accountable for effective management of cyber security risk and key personnel involved in functions relating to the management of cyber security risk (such as information technology and security, business units and operations, risk management, business continuity management and internal audit);

(d) Processes and procedures for the identification, detection, assessment, prioritisation, containment, response to, and escalation of cyber security breaches for decision-making;

CRA-5.8 Cyber Security (continued)

(e) Processes and procedures for the management of outsourcing, system development and maintenance arrangements with third-party service providers, including requirements for such third-party service providers to comply with the licensee's cyber security risk policy;

(f) Communication procedures that will be activated by the licensee in the event of a cyber security breach, which include reporting procedures, information to be reported, communication channels, list of internal and external stakeholders and communication timeline; and

(g) Other key elements of the information security and cyber security risk management including the following:
  (i) information security;
  (ii) data governance and classification;
  (iii) access controls;
  (iv) business continuity and disaster recovery planning and resources;
  (v) capacity and performance planning;
  (vi) systems operations and availability concerns;
  (vii) systems and network security;
  (viii) systems and application development and quality assurance;
  (ix) physical security and environmental controls;
  (x) client data privacy;
  (xi) vendor and third-party service provider management;
  (xii) monitoring and implementing changes to core protocols not directly controlled by the licensee, as applicable;
  (xiii) incident response; and
  (xiv) System audit.

CRA-5.8.6 [This Paragraph was deleted in XX 2023].

CRA-5.8.7 [This Paragraph was deleted in XX 2023].

CRA-5.8 Cyber Security (continued)

Prevention

CRA-5.8.8 A licensee must conduct regular assessments as part of the licensee's compliance programme to identify potential vulnerabilities and cyber security threats in its operating environment which could undermine the security, confidentiality, availability and integrity of the information assets, systems and networks.

CRA-5.8.9 The assessment of the vulnerabilities of the licensee's operating environment must be comprehensive, including making an assessment of potential vulnerabilities relating to the personnel, parties with whom a licensee deals with, systems and technologies adopted, business processes and outsourcing arrangements.

CRA-5.8.10 A licensee must develop and implement preventive measures to minimise the licensee's exposure to cyber security risk.

CRA-5.8.11 Preventive measures referred to in Paragraph CRA-5.8.10 above must include, at a minimum, the following:

(a) Deployment of End Point Protection (EPP) and End Point Detection and Response (EDR) including anti-virus software and malware programs to detect, prevent and isolate malicious code;
(b) Layering systems and systems components;
(c) Use of firewalls for network segmentation including use of Web Application Firewalls (WAF), where relevant, for filtering and monitoring HTTP traffic between a web application and the Internet, and access control lists to limit unauthorized system access between network segments;
(d) Rigorous testing at software development stage as well as after deployment to limit the number of vulnerabilities;
(e) Penetration testing of existing systems and networks;
(f) Use of authority matrix to limit privileged internal or external access rights to systems and data;
(g) Use of a secure email gateway to limit email based cyber attacks such as malware attachments, malicious links, and phishing scams (for example use of Microsoft Office 365 Advanced Threat Protection tools for emails);

CRA-5.8 Cyber Security (continued)

(h) Use of a Secure Web Gateway to limit browser based cyber-attacks, malicious websites and enforce organization policies;

(i) Creating a list of whitelisted applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on the organization's systems; and

(j) Implementing Bring Your Own Device "BYOD" security policies to secure all mobile devices with any access to licensee systems, applications, and networks through security measures such as encryption, remote wipe capabilities, and password enforcement.

CRA-5.8.11A Licensees should also implement the following prevention controls in the following areas:

(a) Data leakage prevention to detect and prevent confidential data from leaving the licensee's technology environment;

(b) Controls to secure physical network ports against connection to computers which are unauthorised to connect to the licensee's network or which do not meet the minimum-security requirements defined for licensee computer systems (e.g. Network access control); and

(c) Identity and access management controls to limit the exploitation and monitor the use of privileged and non-privileged accounts.

CRA-5.8.11B Licensees must set up anti-spam and anti-spoofing measures to authenticate the licensee's mail server and to prove to ISPs, mail services and other receiving mail servers that senders are truly authorized to send the email. Examples of such measures include:

(a) SPF "Sender Policy Framework";

(b) DKIM "Domain Keys Identified Mail"; and

(c) DMARC "Domain-based Message Authentication, Reporting and Conformance".

CRA-5.8.11C Licensees should subscribe to one of the Cyber Threat Intelligence services in order to stay abreast of emerging cyber threats, cybercrime actors and state of the art tools and security measures.

CRA-5.8.11D Licensees must use a single unified private email domain or its subdomains for communication with clients to prevent abuse by third parties. Licensees must not utilise third-party email provider domains for communication with clients. The email domains must comply with the requirements of Paragraph OM-5.8.11B with respect to SPF, DKIM and DMARC.

CRA-5.8 Cyber Security (continued)

CRA-5.8.11E For the purpose of Paragraph CRA-5.8.11D, licensees with subsidiaries or branches outside Bahrain will be allowed to use additional domains subject to CBB's review. Licensees may be allowed, subject to CBB's review, for their clients to receive emails from third-party service providers for specific services offered by such third-parties provided the clients were informed and agreed on such an arrangement. Examples of such third-party services include informational subscription services and document management services.

CRA-5.8.11F **Licensees must comply with the following requirements with respect to URLs or other clickable links in communications with clients:**

(a) Limit the use of links in SMS and other short messages (such as WhatsApp) to messages sent as a result of client request or action. Examples of such client actions include verification links for client onboarding, payment links for client-initiated transactions etc;

(b) Refrain from using shortened links in communication with clients;

(c) Implement measures to allow clients to verify the legitimacy of the links which may include:

(i) clear instructions on the licensee's website/app where the link is sent as a result of client action on the licensee's website/app;

(ii) communication with client such as a phone call informing the client to expect a link from the licensee;

(iii) provision of transaction details such as the transaction amount and merchant name in the message sent to the client with the link;

(iv) use of other verification measures like OTP, password or biometric authentication; and

(d) Create client awareness campaigns to educate their clients on the risk of fraud related to links they receive in SMS, short messages and emails with clear instructions to clients that licensees will not send clickable links in SMS, emails and other short messages to request information or payments unless it is as a result client request or action. Licensees may also train their clients by sending fake phishing messages.

CRA-5.8.12 **[This Paragraph was deleted in XX 2023].**

CRA-5.8 Cyber Security (continued)

CRA-5.8.13 **[This Paragraph was deleted in XX 2023].**

Cyber Risk Identification and Assessments

CRA-5.8.13A **Licensees must conduct periodic assessments of cyber threats. For the purpose of analysing and assessing current cyber threats relevant to the licensee, it should take into account the factors detailed below:**

(a) Cyber threat entities including cyber criminals, cyber activists, insider threats;

(b) Methodologies and attack vectors across various technologies including cloud, email, websites, third parties, physical access, or others as relevant;

(c) Changes in the frequency, variety, and severity of cyber threats relevant to the region;

(d) Dark web surveillance to identify any plot for cyber attacks;

(e) Examples of cyber threats from past cyber-attacks on the licensee where applicable; and

(f) Examples of cyber threats from recent cyber-attacks on other organisations.

CRA-5.8.13B **Licensees must conduct periodic assessments of the maturity, coverage, and effectiveness of all cyber security controls. Cyber security control assessment must include an analysis of the controls' effectiveness in reducing the likelihood and probability of a successful attack.**

CRA-5.8.13C Licensees should ensure that the periodic assessments of cyber threats and cyber security controls cover all critical technology systems. A risk treatment plan should be developed for all residual risks which are considered to be above the licensee's risk tolerance levels.

CRA-5.8.13D **Licensees must conduct regular technical assessments to identify potential security vulnerabilities for systems, applications, and network devices. The vulnerability assessments must be comprehensive and cover internal technology, external technology, and connections with third parties. Preferably, monthly assessments should be conducted for internal technology and weekly or more frequent assessments for external public facing services and systems.**

CRA-5.8.13E With respect to Paragraph CRA-5.8.13D, external technology refers to the licensee's public facing technology such as websites, apps and external servers. Connections with third parties includes any API or other connections with fintech companies, technology providers, outsourcing service providers etc.

CRA-5.8 Cyber Security (continued)

CRA-5.8.13F **Licensees must have in place vulnerability and patch management processes which include remediation processes to ensure that the vulnerabilities identified are addressed and that security patches are applied where relevant within a timeframe that is commensurate with the risks posed by each vulnerability.**

CRA-5.8.13G **All licensees must perform vulnerability assessment and penetration testing of their systems, applications, and network devices to verify the robustness of the security controls in place at least twice a year. These tests must be used to simulate real world cyber-attacks on the technology environment and must:**

(a) Follow a risk-based approach based on an internationally recognized methodology, such as National Institute of Standards and Technology "NIST" and Open Web Application Security Project "OWASP";

(b) Include both Grey Box and Black Box testing in its scope;

(c) Be conducted by qualified and experienced security professionals who are certified in providing penetration testing services;

(d) Be performed internally at periodic intervals by employees having adequate expertise and competency in such testing;

(e) Be performed, twice a year, by external independent third parties who are rotated out at least every two years; and

(f) Be performed on either the production environment or on non-production exact replicas of the production environment.

CRA-5.8.13H The CBB may require additional third-party security reviews to be performed as needed.

CRA-5.8.13I **The time period between two consecutive penetration test and the vulnerability assessment by an independent third party, referred to in Paragraph CRA-5.8.13G(e) must be 6 months and the report on such testing must be provided to CBB within two months following the end of the month where the testing took place. The vulnerability assessment and penetration testing reports must include the vulnerabilities identified and a full list of 'passed' tests and 'failed' tests together with the steps taken to mitigate the risks identified.**

CRA-5.8 Cyber Security (continued)

Cyber Incident Detection and Management

CRA-5.8.14 **[This Paragraph was deleted in XX 2023].**

CRA-5.8.14A **Licensees must implement cyber security incident management processes to ensure timely detection, response and recovery for cyber security incidents. This includes implementing a monitoring system for log correlation and anomaly detection.**

CRA-5.8.14B Licensees should receive data on a real time basis from all relevant systems, applications, and network devices including operational and business systems. The monitoring system should be capable of identifying indicators of cyber incidents and initiate alerts, reports, and response activities based on the defined cyber security incident management process.

CRA-5.8.14C Licensees should retain the logs and other information from the monitoring system for detecting cyber incidents, including "low-and-slow" attacks, in order to facilitate incident investigations, for 12 months or longer.

CRA-5.8.14D Once a cyber incident is detected, licensees should activate their containment measures, processes and technologies best suited to each type of cyber incident to prevent a cyber incident from inflicting further damage. This may involve, after considering the costs, business impact and operational risks, shutting down or isolating all or affected parts of their systems and networks as deemed necessary for containment and diagnosis.

CRA-5.8.14E **Licensees must define roles and responsibilities and assign adequate resources to detect, identify, investigate and respond to cyber incidents that could impact the licensee's infrastructure, services and clients. Such responsibilities must include log correlation, anomaly detection and maintaining the licensee's asset inventory and network diagrams.**

CRA-5.8.14F **Licensees must regularly identify, test, review and update current cyber security risk scenarios and the corresponding response plan. This is to ensure that the scenarios and response plan remain relevant and effective, taking into account changes in the operating environment, systems or the emergence of new cyber security threats. If any gaps are identified, the monitoring system must be updated with new use cases and rule sets which are capable of detecting the current cyber incident scenarios.**

CRA-5.8 Cyber Security (continued)

CRA-5.8.14G The cyber incident scenario tests should include high-impact-low-probability events and scenarios that may result in failure. Common cyber incident scenarios include distributed denial of service (DDoS) attacks, system intrusion, data exfiltration and system disruption. Licensees should regularly use threat intelligence to update the scenarios so that they remain current and relevant. Licensees should periodically review current cyber incident scenarios for the purpose of assessing the licensee's ability to detect and respond to these scenarios if they were to occur.

CRA-5.8.14H Licensees must ensure that critical cyber security incidents detected are escalated to an incident response team, management and the Board, in accordance with the licensee's business continuity plan and crisis management plan, and that an appropriate response is implemented promptly. See also Paragraph CRA-5.8.33 for the requirement to report to the CBB.

CRA-5.8.14I Licensees should clearly define the roles, responsibilities and accountabilities for cyber incident detection and response activities to one or more named individuals that meet the pre-requisite role requirements. Potential conflicts of interest are minimised by ensuring a separation of implementation and oversight roles where possible. The roles should include:

(a) **Incident Owner:** An individual who is responsible for handling the overall cyber incident detection and response activities according to the incident type and services affected. The Incident Owner is delegated appropriate authority to manage the mitigation or preferably, removal of all impacts due to the incident.

(b) **Spokesperson:** An individual, who is responsible for managing the communications strategy by consolidating relevant information and views from subject matter experts and the licensee's management to update the internal and external stakeholders with consistent information.

(c) **Record Keeper:** An individual who is responsible for maintaining an accurate record of the cyber incident throughout its different phases, as well as documenting actions and decisions taken during and after a cyber incident. The record should serve as an accurate source of reference for after-action reviews to improve future cyber incident detection and response activities.

CRA-5.8.14J For the purpose of managing a critical cyber incident, the licensee should operate a situation room, and should include in the incident management procedure a definition of the authorities and responsibilities of staff members, internal and external reporting lines, communication channels, tools and detailed working procedures. The situation room or a war room is a physical room or a virtual room where relevant members of the management gather to handle a crisis in the most efficient manner possible.

CRA-5.8 Cyber Security (continued)

CRA-5.8.14K Licensees should record and document in an orderly manner the incidents that have been handled and the actions that were taken by the relevant functions. In particular, the licensee should maintain an "incident log" in which all the notifications, decisions and actions taken, in relation to cyber incidents, are documented, as close as possible to the time of their occurrence. It should also include the status of the issue whether it is open or has been resolved and the person in charge of resolving the issue/incident. The logs should be stored and preserved in a secure and legally admissible manner.

CRA-5.8.14L Licensees should utilise pre-defined taxonomy for classifying cyber incidents according to, for example, the type of incident, threat actors, threat vectors and repercussions; and a pre-established severity assessment framework to help gauge the severity of the cyber incident. For example, taxonomies that can be used when describing cyber incidents:

(a) Describe the cause of the cyber incident (e.g. process failure, system failure, human error, external event, malicious action).
(b) Describe whether the cyber incident is due to a third-party service provider.
(c) Describe the attack vector (e.g. malware, virus, worm, malicious hyperlink).
(d) Describe the delivery channel used (e.g. e-mail, web browser, removable storage media).
(e) Describe the impact (e.g. service degradation/disruption, service downtime, potential impact to clients, data leakage, unavailability of data, data destruction/corruption, reputational damage).
(f) Describe the type of incident (e.g. zero-day attack, exploiting a known vulnerability, isolated incident).
(g) Describe the intent (e.g. malicious, theft, monetary gain, fraud, political, espionage, opportunistic).
(h) Describe the threat actor (e.g. script kiddies, amateur, criminal syndicate, hacktivist, nation state).

The cyber incident severity may be classified as:

(a) **Severity 1** incident has caused or will cause a serious disruption or degradation of critical service(s) and there is potentially high impact on public confidence in the licensee.
(b) **Severity 2** incident has or will cause some degradation of critical services and there is medium impact on public confidence in the licensee.
(c) **Severity 3** incident has little or no impact to critical services and there is no visible impact on public confidence in the licensee.

CRA-5.8.14M Licensees should determine the effects of the cyber incident on clients and to the wider financial system as a whole and report the results of such an assessment to the CBB if it is determined that the cyber incident may have a systemic impact.

CRA-5.8 Cyber Security (continued)

CRA-5.8.14N Licensees should establish metrics to measure the impact of a cyber incident and to report to management the performance of response activities. Examples include:
(a) Metrics to measure impact of a cyber incident:
(i) Duration of unavailability of critical functions and services;
(ii) Number of stolen records or affected accounts;
(iii) Volume of clients impacted;
(iv) Amount of lost revenue due to business downtime, including both existing and future business opportunities; and
(v) Percentage of service level agreements breached.
(b) Performance metrics for incident management:
(i) Volume of incidents detected and responded via automation;
(ii) Dwell time (i.e. the duration a threat actor has undetected access until completely removed); and
(iii) Recovery Point objectives (RPO) and recovery time objectives (RTO) satisfied.

CRA-5.8.15 **[This Paragraph was deleted in XX 2023].**

CRA-5.8.16 **[This Paragraph was deleted in XX 2023].**

CRA-5.8.17 **[This Paragraph was deleted in XX 2023].**

CRA-5.8.18 **[This Paragraph was deleted in XX 2023].**

CRA-5.8.19 **[This Paragraph was deleted in XX 2023].**

CRA-5.8.19A **[This Paragraph was deleted in XX 2023].**

CRA-5.8.20 **[This Paragraph was deleted in XX 2023].**

CRA-5.8.20A **Licensees must identify the critical systems and services within its operating environment that must be recovered on a priority basis in order to provide certain minimum levels of service during the downtime and determine how much time the licensee will require to return to full service and operations.**

CRA-5.8 Cyber Security (continued)

CRA-5.8.20B Critical incidents are defined as incidents that trigger the BCP and the crisis management plan. Critical systems and services are those whose failure can have material impact on any of the following elements:

(a) Financial situation;
(b) Reputation;
(c) Regulatory, legal and contractual obligations;
(d) Operational aspects; and
(e) Delivery of key products and services.

CRA-5.8.20C Licensees must define a program for recovery activities for the purpose of timely restoration of any capabilities or services that were impaired due to a cyber security incident. Licensees must establish recovery time objectives ("RTOs"), i.e. the time within which the intended process is to be covered, and recovery point objectives ("RPOs"), i.e. point to which information used must be restored to enable the activity to operate on resumption. Licensees must also consider the need for communication with third party service providers, clients and other relevant external stakeholders as may be necessary.

CRA-5.8.20D Licensees must ensure that all critical systems are able to recover from a cyber security breach within the licensee's defined RTO in order to provide important services or some level of minimum services for a temporary period of time.

CRA-5.8.20E Licensees should validate that recovered assets are free of compromise, fully functional and meet the security requirements before returning the systems to normal business operations. This includes performing checks on data to ensure data integrity. In some cases, licensees may need to use backup data kept in a disaster recovery site or plan for the reconstruction of data from external stakeholders such as business partners and clients.

CRA -5.8.20F Licensees must define a program for exercising the various response mechanisms, taking into account the various types of exercises such as attack simulations, "war games" and "tabletop" exercises, and with reference to the relevant stakeholders such as technical staff, crisis management team, decision-makers and spokespersons.

CRA-5.8.20G Licensees must define the mechanisms for ensuring accurate, timely and actionable communication of cyber incident response and recovery activities with the internal stakeholders, including to the board or designated committee of the board.

CRA-5.8 Cyber Security (continued)

CRA-5.8.21 **[This Paragraph was deleted in XX 2023].**

CRA-5.8.22 **A licensee must ensure its business continuity plan is comprehensive and includes a recovery plan for its systems, operations and services arising from a cyber security incident breach.**

Chief Information Security Officer

CRA-5.8.23 **A licensee's CISO, as referred to in Paragraph CRA-5.8.3(d), is responsible for overseeing and implementing the licensee's cyber security program and enforcing its cyber security policy. The CISO must report to an independent risk management function or the licensee must incorporate the responsibilities of cyber security risk into the risk management function.**

CRA-5.8.24 **[This Paragraph was deleted in January 2020].**

IT System Audit

CRA-5.8.25 **[This Paragraph was deleted in January 2020].**

CRA-5.8.25A **[This Paragraph was deleted in XX 2023].**

CRA-5.8.26 **[This Paragraph was deleted in XX 2023].**

CRA-5.8.27 **[This Paragraph was deleted in XX 2023].**

Cyber Risk Insurance

CRA-5.8.28 **A licensee, based on the assessment of cyber security risk exposure and with an objective to mitigate cyber security risk, must evaluate and consider the option of availing cyber risk insurance. The evaluation process to determine suitability of cyber risk insurance as a risk mitigant must be undertaken on a yearly basis and be documented by the licensee.**

CRA-5.8.29 The cyber risk insurance policy, referred to in Paragraph CRA-5.8.28, may include some or all of the following types of coverage, depending on the risk assessment outcomes:

(a) Crisis management expenses, such as costs of notifying affected parties, costs of forensic investigation, costs incurred to determine the existence or cause of a breach, regulatory compliance costs, costs of analysing the licensee's legal response obligations;

CRA-5.8 Cyber Security (continued)

(a) Claim expenses such as costs of defending lawsuits, judgments and settlements, and costs of responding to regulatory investigations;
(b) Coverage for a variety of torts, including invasion of privacy or copyright infringement; and
(c) Coverages relating to loss of revenue due to interruption of data systems resulting from a cyber or denial of service attack and other costs associated with the loss of data collected by the licensee.

Training and Awareness

CRA-5.8.30 **Licensees must evaluate improvement in the level of awareness and preparedness to deal with cyber security risk to ensure the effectiveness of the training programmes implemented.**

CRA-5.8.31 **The licensee must ensure that all employees receive adequate training on a regular basis, in relation to cyber security and the threats they could encounter, such as through testing employee reactions to simulated cyber-attack scenarios. All relevant employees must be informed on the current cyber security breaches and threats. Additional training should be provided to 'higher risk staff'.**

CRA-5.8.32 **The licensees must ensure that role specific cyber security training is provided on a regular basis to relevant staff including:**
(a) Executive board and senior management;
(b) Cyber security roles;
(c) IT staff; and
(d) Any high-risk staff as determined by the licensee.

Reporting to the CBB

CRA-5.8.33 **Upon occurrence or detection of any cyber security incident or detection of any unplanned outages, whether internal or external, that compromises client information or disrupts critical services that affect operations, licensees must contact the CBB, immediately (within one hour), on 17547477 and submit Section A of the Cyber Security Incident Report (Appendix-B) to the CBB's cyber incident reporting email, incident.cra@cbb.gov.bh, as soon as possible, but not later than two hours, following occurrence or detection of any cyber incidents.**

CRA-5.8 Cyber Security (continued)

CRA-5.8.34 **Following the submission referred to in Paragraph CRA 5.8.33, the licensee must submit to the CBB Section B of the Cyber Security Incident Report (Appendix B) within 10 calendar days of the occurrence of the cyber security incident. Licensees must include all relevant details in the report, including the full root cause analysis of the cyber security incident, its impact on the business operations and clients, and all measures taken by the licensee to stop the attack, mitigate its impact and to ensure that similar events do not recur. In addition, a weekly progress update must be submitted to CBB until the incident is fully resolved.**

CRA-5.8.35 With regards to the submission requirement mentioned in Paragraph CRA-5.8.34, the licensee should submit the report with as much information as possible even if all the details have not been obtained yet.

CRA-5.8.36 **The vulnerability assessment and penetration testing report (see Paragraph CRA-5.8.13I), along with the steps taken to mitigate the risks must be maintained by the licensee for a five-year period from the date of the report.**

CRA-6.1 Board of Directors' Responsibility

CRA-6.1.1 **The Board of Directors of licensees are responsible for the establishment of an adequate and effective framework for identifying, monitoring and managing risks across all its operations.**

CRA-6.1.2 The CBB expects the Board to be able to demonstrate that it provides suitable oversight and establishes, in relation to all the risks the licensee is exposed to, a risk management framework that includes setting and monitoring policies, systems, tools and controls.

CRA-6.1.3 Although authority for the management of a firm's risks is likely to be delegated, to some degree, to individuals at all levels of the organisation, the overall responsibility for this activity should not be delegated from its governing body and relevant senior managers.

CRA-6.1.4 A licensee's failure to establish, in the opinion of the CBB, an adequate risk management framework will result in it being in breach of Condition 6 of the Licensing Conditions. This failure may result in the CBB withdrawing or imposing restrictions on the licensee, or the licensee being required to inject more capital.

CRA-6.1.5 The Board of Directors must also ensure that there is adequate documentation of the licensee's risk management framework.

Systems and Controls

CRA-6.1.6 **The risk management framework of licensees must provide for the establishment and maintenance of effective systems and controls as are appropriate to their business, so as to identify, measure, monitor and manage risks.**

CRA-6.1.7 An effective framework for risk management should include systems to identify, measure, monitor and control all major risks on an on-going basis. The risk management systems should be approved and periodically reviewed by the Board.

CRA-6.1.8 **The systems and controls required under Paragraph CRA-6.1.6 must be proportionate to the nature, scale and complexity of the licensee's activities.**

CRA-6.1 Board of Directors' Responsibility (continued)

CRA-6.1.9 **The processes and systems required must enable the licensee to identify the major sources of risk to its ability to meet its liabilities as they fall due, including the major sources of risk in each of the following categories:**

(a) Counterparty risk;
(b) Market risk;
(c) Liquidity risk;
(d) Operational risk including cyber security risk;
(e) Outsourcing risk;
(f) Group risk; and
(g) Any additional categories relevant to its business.

CRA-6.1.10 **Licensees must establish and maintain a risk management function that operates independently and which has sufficient authority and resources, including access to the Board of Directors, to facilitate the carrying out of the following tasks:**

(a) The implementation of the risk management framework and maintenance of effective systems and controls referred to in Paragraph CRA-6.1.6;
(b) The provision of reports and advice to senior management;
(c) The development of the licensee's risk strategy; and
(d) Direct communication with the Board of Directors, independently from the licensee's senior management, regarding concerns, where specific risk developments affect or may affect the licensee, without prejudice to the responsibilities of the Board of Board in its supervisory and/or managerial functions.

CRA-6.1.11 The CBB may permit a licensee to establish and maintain a risk management function which does not operate independently, provided this does not give rise to conflicts of interest and the licensee demonstrates to the CBB that the establishment and maintenance of a dedicated independent risk management function with sole responsibility for the risk management function is not appropriate and proportionate in view of the nature, scale and complexity of its business and the nature and range of the regulated crypto-asset services undertaken in the course of that business.

CRA-6.1.12 Where a licensee is granted an exemption referred to in Paragraph CRA-6.1.11, the licensee must nevertheless be able to demonstrate that the policies and procedures which it has adopted in accordance with Paragraph CRA-6.1.6 satisfy the requirements thereof and are consistently effective.

CRA-6.2 Counterparty Risk

CRA-6.2.1 Licensees must adequately document the necessary policies and procedures for identifying, measuring, monitoring and controlling counterparty risk. This policy must be approved by the Board of Directors and regularly reviewed by the senior management of the licensee.

CRA-6.2.2 Among other things, the licensee's policies and procedures must identify the limits it applies to counterparties, how it monitors movements in counterparty risk and how it mitigates loss in the event of counterparty failure.

CRA-6.3 Market Risk

CRA-6.3.1 Licensees must document their framework for the proactive management of market risk for accepted crypto-assets. This policy must be approved by the Board of Directors and regularly reviewed by the senior management of the licensee.

CRA-6.3.2 Licensees must ensure that clients, before undertaking transactions, pre-fund their accounts.

CRA-6.3.3 Licensees must not provide any financial assistance to clients to acquire or undertake a transaction in crypto-assets.

CRA-6.4 Liquidity Risk

CRA-6.4.1 Licensees must maintain a liquidity risk policy for the management of liquidity risk, which is commensurate to the nature, scale and complexity of its activities. This policy must be approved by the Board of Directors and regularly reviewed by the senior management of the licensee.

CRA-6.4.2 Among other things, the licensee's liquidity risk policy must identify the limits it applies, how it monitors movements in risk and how it mitigates loss in the event of unexpected liquidity events.

CRA-6.5 Operational Risk

CRA-6.5.1 **Licensees must document their framework for the proactive management of operational risk. This policy must be approved by the Board of Directors and regularly reviewed by the senior management of the licensee.**

CRA-6.5.2 **Licensees must consider the impact of operational risks on their financial resources and solvency.**

CRA-6.5.2A **Licensees must identify possible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability including having adequate capacity.**

CRA-6.5.2B **Licensees must, among other things:**

(a) Establish a robust operational risk-management framework with appropriate systems, policies, procedures, and controls to identify, monitor, mitigate and manage operational risks;

(b) Have in place clearly defined roles and responsibilities for addressing operational risk;

(c) Have in place clearly defined operational reliability objectives and have policies in place that are designed to achieve those objectives;

(d) Ensure that it has adequate capacity proportionate to stress volumes to achieve its service-level objectives; and

(e) Have a comprehensive physical and information security policy that addresses all potential vulnerabilities and threats.

CRA-6.5.3 **Licensees' business continuity planning, risk identification and reporting must cover reasonably foreseeable external events and their likely impact on the licensee and its business portfolio.**

CRA-6.5.4 Business continuity management includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Its purpose is to minimise the operational, financial, legal, reputational and other material consequences arising from a disruption. Effective business continuity management concentrates on the impact, as opposed to the source, of the disruption, which affords financial industry participants and financial authorities greater flexibility to address a broad range of disruptions. At the same time, however, licensees should not ignore the nature of risks to which they are exposed.

CRA-6.5 Operational Risk (continued)

Business Continuity and Disaster Recovery

CRA-6.5.5 Licensees must establish and maintain a written business continuity and disaster recovery plan reasonably designed to ensure the availability and functionality of the Licensee's services in the event of an emergency or other disruption to the Licensee's normal business activities. The business continuity and disaster recovery plan, at minimum, must:

(a) Identify documents, data, facilities, infrastructure, personnel, and competencies essential to the continued operations of the Licensee's business;

(b) Identify the supervisory personnel responsible for implementing each aspect of the business continuity and disaster recovery plan; include a plan to communicate with essential Persons in the event of an emergency or other disruption to the operations of the Licensee, including employees, counterparties, regulatory authorities, data and communication providers, disaster recovery specialists, and any other Persons essential to the recovery of documentation and data and the resumption of operations;

(c) Include procedures for the maintenance of back-up facilities, systems, and infrastructure as well as alternative staffing and other resources to enable the timely recovery of data and documentation and to resume operations as soon as reasonably possible following a disruption to normal business activities;

(d) Include procedures for the back-up or copying, with sufficient frequency, of documents and data essential to the operations of the Licensee and storing of the information off site; and

(e) Identify third parties that are necessary to the continued operations of the Licensee's business.

CRA-6.5.6 Licensees must distribute a copy of the business continuity and disaster recovery plan, and any revisions thereto, to all relevant employees and must maintain copies of the business continuity and disaster recovery plan at one or more accessible off-site locations.

CRA-6.5.7 Licensees must provide relevant training to all employees responsible for implementing the business continuity and disaster recovery plan regarding their roles and responsibilities.

CRA-6.5.8 Licensees must immediately notify the CBB of any emergency or other disruption to its operations that may affect its ability to fulfil regulatory obligations or that may have a significant adverse effect on the Licensee, its counterparties, or the market.

CRA-6.5 Operational Risk (continued)

CRA-6.5.9 The business continuity and disaster recovery plan must be tested at least annually by qualified, independent internal personnel or a qualified third party, and revised accordingly.

CRA-6.6 Outsourcing Arrangements

CRA-6.6.1 **This Chapter sets out the CBB's approach to outsourcing by licensees. It also sets out various requirements that licensees must address when considering outsourcing an activity or function.**

CRA-6.6.2 In the context of this Chapter, 'outsourcing' means an arrangement whereby a third party performs on behalf of a licensee an activity which commonly would have been performed internally by the licensee. Examples of services that are typically outsourced include data processing, cloud services, customer call centres and back-office related activities.

CRA-6.6.3 In the case of branches of foreign entities, the CBB may consider a third-party outsourcing arrangement entered into by the licensee's head office/regional office or other offices of the foreign entity as an intragroup outsourcing, provided that the head office/regional office submits to the CBB a letter of comfort which includes, but is not limited to, the following conditions:

(i) The head office/regional office declares its ultimate responsibility of ensuring that adequate control measures are in place; and

(ii) The head office/regional office is responsible to take adequate rectification measures, including compensation to the affected customers, in cases where customers suffer any loss due to inadequate controls applied by the third-party service provider.

CRA-6.6.4 **The licensee must not outsource the following functions:**

(i) Compliance;

(ii) AML/CFT;

(iii) Financial control;

(iv) Risk management; and

(v) Business line functions offering regulated services directly to the customers (refer to Regulation No. (1) of 2007 and its amendments for the list of CBB regulated services).

CRA-6.6.5 **For the purposes of Paragraph CRA-6.6.4, certain support activities, processes and systems under these functions may be outsourced (e.g. call centres, data processing, credit recoveries, cyber security, e-KYC solutions) subject to compliance with Paragraph CRA-6.6.7. However, strategic decision-making and managing and bearing the principal risks related to these functions must remain with the licensee.**

CRA-6.6.6 Branches of foreign entities may be allowed to outsource to their head office, the risk management function stipulated in Subparagraph CRA-6.6.4 (iv), subject to CBB's prior approval.

CRA-6.6 Outsourcing Arrangements (continued)

CRA-6.6.7 Licensees must comply with the following requirements:

(i) Prior CBB approval is required on any outsourcing to a third-party outside Bahrain (excluding cloud data services). The request application must:

a. include information on the legal and technical due diligence, risk assessment and detailed compliance assessment; and

b. be made at least 30 calendar days before the licensee intends to commit to the arrangement.

(ii) Post notification to the CBB, within 5 working days from the date of signing the outsourcing agreement, is required on any outsourcing to an intragroup entity within or outside Bahrain or to a third-party within Bahrain, provided that the outsourced service does not require a license, or to a third-party cloud data services provider inside or outside Bahrain.

(iii) Licensees must have in place sufficient written requirements in their internal policies and procedures addressing all strategic, operational, logistical, business continuity and contingency planning, legal and risks issues in relation to outsourcing.

(iv) Licensees must sign a service level agreement (SLA) or equivalent with every outsourcing service provider. The SLA must clearly address the scope, rights, confidentiality and encryption requirements, reporting and allocation of responsibilities. The SLA must also stipulate that the CBB, external auditors, internal audit function, compliance function and where relevant the Shari'a coordination and implementation and internal Shari'a audit functions of the licensee have unrestricted access to all relevant information and documents maintained by the outsourcing service provider in relation to the outsourced activity.

(v) Licensees must designate an approved person to act as coordinator for monitoring and assessing the outsourced arrangement.

(vi) Licensee must submit to the CBB any report by any other regulatory authority on the quality of controls of an outsourcing service provider immediately after its receipt or after coming to know about it.

(vii) Licensee must inform its normal supervisory point of contact at the CBB of any material problems encountered with the outsourcing service provider if they remain unresolved for a period of three months from its identification date.

CRA-6.6 Outsourcing Arrangements (continued)

CRA-6.6.8 For the purpose of Subparagraph CRA-6.6.7 (iv), licensees as part of their assessments may use the following:

(a) Independent third-party certifications on the outsourcing service provider's security and other controls;
(b) Third-party or internal audit reports of the outsourcing service provider; and
(c) Pooled audits organized by the outsourcing service provider, jointly with its other clients.

When conducting on-site examinations, licensees should ensure that the data of the outsourcing service provider's other clients is not negatively impacted, including impact on service levels, availability of data and confidentiality.

CRA-6.6.9 For the purpose of Subparagraph CRA-6.1.7 (i), the CBB will provide a definitive response to any prior approval request for outsourcing within 10 working days of receiving the request complete with all the required information and documents.

CRA-7.1 [This Chapter was deleted in XX 2023]

CRA-7.1.1 [This Paragraph was deleted in XX 2023].

CRA-7.1.1A [This Paragraph was deleted in XX 2023].

CRA-7.1.2 [This Paragraph was deleted in January 2020].

CRA-7.1.3 [This Paragraph was deleted in XX 2023].

CRA-7.1.4 [This Paragraph was deleted in XX 2023].

CRA-7.1.5 [This Paragraph was deleted in XX 2023].

CRA-8.1 General Requirements

CRA-8.1.1 This Section applies to licensees that undertake safeguarding, storing, holding or maintaining custody of crypto-assets as specified in Paragraph CRA-1.1.6(e).

CRA-8.1.2 [This Paragraph was deleted in XX 2023].

CRA-8.1.3 A licensee which undertakes safeguarding, storing, holding or maintaining custody of crypto-assets must have systems and controls in place to:

(a) Ensure the proper safeguarding of crypto-assets;

(b) Ensure that such safe custody of crypto-assets is identifiable and secure at all times; and

(c) Ensure protection against the risk of loss, theft or hacking.

CRA-8.1.4 [This Paragraph was deleted in XX 2023].

CRA-8.1.5 To the extent a licensee stores, holds, or maintains custody or control of crypto-asset on behalf of a client, such licensee must hold crypto-asset of the same type and amount as that which is owed or obligated to such other client.

CRA-8.1.6 A licensee is prohibited from selling, transferring, assigning, lending, hypothecating, pledging, or otherwise using or encumbering crypto-asset stored, held, or maintained by, or under the custody or control of, such licensee on behalf of a client except for the sale, transfer, or assignment of such crypto-asset at the direction of the client.

CRA-8.1.7 A licensee that maintains custody or control of crypto-asset must avoid conflict of interest between its function as a crypto-asset custodian and any other activities. With an objective to avoid or mitigate actual or potential conflict of interest between its custody function and any other activities, the licensee must adopt a governance structure that ensures adequate management of conflicts of interest crypto-asset custody activity is fully independent from its other activities. Such governance structure must include, among other things, having separate staffing arrangements to undertake the crypto-asset custody activity, who do not have any conflicting responsibilities within the licensee's other activities.

CRA-8.1 General Requirements (continued)

CRA-8.1.8 A licensee that maintains custody or control of crypto-assets on behalf of a client must store, at a minimum, 90% of client's crypto-assets in cold wallets to minimise exposure to losses arising from a compromise or hacking. The requirement to hold 90% of client's crypto-assets in cold wallet is to be calculated separately for each crypto-asset that is listed on the licensee's platform and not at aggregate level.

CRA-8.1.9 A licensee must have a documented policy detailing the mechanism for the transfer of crypto-assets between hot, cold and other storage. The scope of authority of each function designated to perform any non-automated processes in such transfers must be clearly specified in the policy document.

Multi-Signature Arrangement

CRA-8.1.10 A licensee that maintains custody or control of crypto-assets must not, at any time, permit arrangements whereby just a party or signatory is able to completely authorise the movement, transfer or withdrawal of crypto assets held under custody on behalf of clients. In particular, licensees must not have custody arrangements whereby only a sole person can fully access the private key or keys for the crypto assets held under custody by the licensee.

CRA-8.1.11 Licensees that maintain custody or control of crypto-assets are required to mitigate the risk of collusion between the authorised persons or signatories who are able to authorise the movement, transfer or withdrawal of crypto-assets held under custody.

Other Requirements

CRA-8.1.12 Licensees that maintain custody or control of crypto-assets 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 crypto assets held under custody on behalf of clients. In addition, licensees must have clearly defined policies and procedures to enable or revoke the authority granted to these persons.

CRA-8.1 General Requirements (continued)

CRA-8.1.13 Licensees that maintain custody or control of crypto-assets are required to have policies and procedures in place that clearly describe the process that will be adopted in the event that the licensee comes to know or suspects that the crypto assets it is holding under custody on behalf for clients have been compromised, such as in the event of a hacking attack, theft or fraud. Such policies and procedures must detail the specific steps the licensee will take to protect client's crypto assets in the event of such incidents. Licensees must also have the ability to immediately halt all further transactions with regard to the crypto assets.

Forks and Air Drops

CRA-8.1.14 Licensees must have written procedures for dealing with events such as forks (hard, soft or temporary forks) or air drops from an operational and technical point of view.

CRA-8.1.15 Where a licensee supports a new protocol, it must 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.

CRA-8.1.16 Where a licensee supports a new protocol, a licensee must ensure that their clients are able to deposit and withdraw crypto-assets in and out of the wallet as and when requested before and after a fork (except during go-live). Clients must be notified well in advance of any periods of time when deposits and withdrawals are not feasible.

CRA-8.1.17 Where the underlying protocol of a crypto-asset is changed, and the older version of the 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), a licensee, where it supports a new protocol, must ensure that client balances on the old version are reconciled with the new version of the crypto-asset. This includes availability of reverse compatibility for as long as required. A licensee must maintain transparent lines of communication with their clients on how they are managing clients crypto-asset holdings in such a scenario.

CRA-8.1 General Requirements (continued)

CRA-8.1.18 In the case of a hard fork, a licensee, where it supports a new protocol, must proactively manage any discrepancy between the balances recorded on the previous version versus the new version by engaging with the entity which is responsible for updating and supporting the underlying protocol of the relevant crypto-asset. Additionally, licensees must 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 a crypto-asset and that they notify the CBB well in advance of offering the new crypto-asset as part of their activities.

CRA-8.2 Custodial Arrangements

CRA-8.2.1 Licensees must provide to the CBB, for prior written approval, details of custodial arrangement put in place to safeguard, store, hold or maintain custody of crypto-assets.

CRA-8.2.2 Licensees may implement the following three types of custodial arrangements or any other type of custodial arrangement that is acceptable to the CBB:

(a) The licensee is wholly responsible for custody of client's crypto-assets and provides this service "in-house" through its own crypto-assets wallet solution. Such an arrangement includes scenarios where a licensee provides its own in-house proprietary wallet for clients to store any crypto-assets bought through that licensee or transferred into the wallet from other sources.

(b) The licensee 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 licensee uses a third-party service provider to hold all its clients' accepted crypto-assets (e.g., all or part of the clients' private keys).

(c) The licensee wholly allows clients to "self-custodise" their accepted crypto-assets. Such an arrangement includes scenarios where licensees require clients to self-custodise their crypto-assets. Such licensees only provide the 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 licensee have no control over or responsibility for). This arrangement also includes the scenario where licensees 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 licensee does not control).

CRA-8.2 Custodial Arrangements

Third Party Crypto-asset Custody Arrangement

CRA-8.2.3 **For the purposes of Paragraph CRA-8.2.2(b), where a licensee provides a third party crypto-asset custodian to a client it must undertake an appropriate risk assessment of that crypto-asset custodian. Licensees must also retain ultimate responsibility for safe custody of crypto-assets held on behalf of clients and ensure that they continue to meet all their regulatory obligations with respect to crypto-asset custody service and outsourced activities.**

CRA-8.2.4 In undertaking an appropriate risk assessment of the third party crypto-asset custodian in accordance with Paragraph CRA-8.2.3, licensees should take into account any or all of the following:

(a) The expertise and market reputation of the third party crypto-asset custodian, and once a crypto-asset has been lodged by the licensee with the third party crypto-asset custodian, the crypto-asset custodian's performance of its services to the licensee;
(b) The arrangements, including cyber security measures, for holding and safeguarding crypto-assets;
(c) An appropriate legal opinion as to the protection of crypto-assets in the event of insolvency of the custodian;
(d) Whether the third party crypto-asset custodian is regulated and by whom;
(e) The capital or financial resources of the third party crypto-asset custodian;
(f) The credit rating of the third party crypto-asset custodian; and
(g) Any other activities undertaken by the third party crypto-asset custodian and, if relevant, any affiliated company

CRA-8.2.5 **When assessing the suitability of the third party crypto-asset custodian, the licensee must ensure that the third party crypto-asset custodian will provide protections equivalent to the protections specified in this Section and applicable client asset and client money protection rules as specified in Chapter CRA-4.5.**

CRA-8.2 Custodial Arrangements

CRA-8.2.6 **A licensee that safeguards, stores, holds or maintains custody of crypto-assets with a third party crypto-asset custodian, must establish and maintain a system for assessing the appropriateness of its selection of the crypto-asset custodian and assess the continued appointment of that crypto-asset custodian periodically as often as is reasonable. The licensee must make and retain a record of the grounds on which it satisfies itself as to the appropriateness of its selection or, following a periodic assessment, continued appropriateness of the crypto-asset custodian.**

CRA-8.2.7 **[This Paragraph was deleted in XX 2023].**

Self-Custody Arrangement

CRA-8.2.8 **For the purposes of Paragraph CRA-8.2.2(c), the CBB 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 the crypto-assets face the constant risk of being stolen by malicious actors. As such, licensees requiring clients to self-custodise crypto-assets are required to disclose this fact fully and clearly upfront to clients and meet the disclosure standards as specified in Paragraph CRA-4.5.8.**

CRA-8.2.9 [This Paragraph was deleted in XX 2023].

CRA-8.3 Crypto Wallets

CRA-8.3.1 **[This Paragraph was deleted in XX 2023].**

CRA-8.3.2 For the purposes of this Section, licensees should consider, at the minimum, the following two types of crypto-asset wallets:

(a) Custodial Wallet: 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. Licensees that hold crypto-assets on behalf of their clients should generally offer custodial wallets and may even offer multi-signature wallets (Paragraph CRA-5.4.5). 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~~.~~; and

(b) Non-Custodial (Self-Custody) Wallets: 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' authorisation.

CRA-8.3.3 In addition to the two main crypto-asset wallet types described in Paragraph CRA-8.3.2 above, the CBB recognises that there may be alternative crypto-asset wallet models in existence or which may emerge in future. Licensees 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 CBB.

CRA-8.3 Crypto Wallets (continued)

CRA-8.3.4 Only entities providing the custodial wallets as described in Paragraph CRA-8.3.2(a) above are considered to be carrying out the regulated activity of safeguarding, storing, holding, maintaining custody of or arranging custody on behalf of clients for crypto-assets as specified in Paragraph CRA-1.1.6(e). With respect to the non-custodial wallets as described in Paragraph CRA-8.3.2(b) above, the wallet provider is merely providing the technology; it is the wallet user himself who has full control of and responsibility for the crypto-assets.

CRA-8.3.5 **[This Paragraph was deleted in XX 2023].**

CRA-8.3.6 **Licensees must assess the risks posed to each storage method in view of the new developments in security threats, technology and market conditions and must implement appropriate storage solutions to ensure the secure storage of crypto-assets held on behalf of clients. Wallet storage technology and any upgrades should be tested comprehensively before deployment to ensure reliability. A licensee must implement and must ensure that its third-party crypto-asset custodian implements, measures to deal with any compromise or suspected compromise of all or part of any seed or private key without undue delay, including the transfer of all client crypto-assets to a new storage location as appropriate.**

CRA-8.3.7 **Licensees must have, or where the licensee uses the service of a third party crypto-asset custodian it must ensure that the third party crypto-asset custodian has, adequate processes in place for handling deposit and withdrawal requests for crypto-asset to guard against loss arising from theft, fraud and other dishonest acts, professional misconduct or omissions. In this regard, a licensee must:**

(a) Continuously monitor major developments (such as technological changes or the evolution of security threats) relevant to all crypto-assets included for trading. There must be clear processes in place to evaluate the potential impact and risks of these developments, as well as processes for handling fraud attempts specific to distributed ledger technology (such as 51% attacks), and these processes should be proactively executed;

(b) Ensure that client IP addresses as well as wallet addresses used for deposit and withdrawal are whitelisted, using appropriate confirmation methods;

CRA-8.3 Crypto Wallets (continued)

(a) Have clear processes in place to minimise the risks relating to handling deposits and withdrawals, including whether deposits and withdrawals are performed using hot or cold storage, whether withdrawals are processed on a real-time basis or only at certain cut-off times, and whether the withdrawal process is automatic or involves manual authorisation;

(b) Ensure that any decision to suspend the withdrawal of crypto-assets is made on a transparent and fair basis, and is communicated without delay to all its clients; and

(c) Ensure that the above processes include safeguards against fraudulent requests or requests made under duress as well as controls to prevent one or more officers or employees from transferring assets to wallet addresses other than the client's designated wallet address.

CRA-8.3.8 Where the licensee appoints a third-party crypto-asset custodian, the licensee must ensure that such custodian implements the above requirements.

CRA-8.4 Reconciliation, Client Reporting and Record Keeping

Reconciliation

CRA-8.4.1 A licensee must at least every calendar month:

(a) [This Subparagraph was deleted in XX 2023];
(b) Reconcile all crypto-assets held by the licensee, or its appointed third party custodian, and reconcile the result to the records of the licensee;
(c) Reconcile individual client balances with the licensee's records of crypto-assets balances held in client accounts; and
(d) Where the licensee discovers discrepancies after carrying out the above reconciliations, it must maintain a record of such discrepancies and the measures taken to remedy such discrepancies.

Client Reporting

CRA-8.4.2 [This Paragraph was deleted in XX 2023].

CRA-8.4.3 [This Paragraph was deleted in XX 2023].

Record Keeping

CRA-8.4.4 A licensee must ensure that proper records of the client's custody account which it holds or receives, or arranges for another to hold or receive, on behalf of the client, are made and retained for a period of ten years after the account is closed.

CRA-8.4 Reconciliation, Client Reporting and Record Keeping (continued)

CRA-8.4.5 For the purpose of Paragraph CRA-8.4.4, the records must capture at a minimum the following details:

(a) The name of the account;
(b) The account number;
(c) Type of account;
(d) The location of the account;
(e) Whether the account is currently open or closed;
(f) Details of crypto-assets held and movements in each account; and
(g) The date of opening and where applicable, closure.

CRA-9.1 [This Chapter was deleted in XX 2023]

CRA-9.1.1 [This Paragraph was deleted in XX 2023].

CRA-10.1 Reporting Requirements

Reports Prepared by a Licensee

CRA-10.1.1 [This Paragraph was deleted in XX 2023].

CRA-10.1.2 Licensees must submit a Professional Indemnity Insurance Return (Form PIIR) on an annual basis (ref. CRA-4.8.1). Additionally, they must provide, upon request, evidence to the CBB of the coverage in force.

CRA-10.1.3 Licensees must submit quarterly to the Consumer Protection Unit at the CBB a report summarising the outcome of their complaint handling procedures in accordance with the requirements of Paragraph CRA-4.7.12.

CRA-10.1.3A Licensees must submit on an annual basis, no later than 2 months from the end of the reporting period, a report on their liquidity partners which must include the liquidity partners' names, information on the total value and volume transacted for each type of crypto-asset, and the percentage of all client orders executed through the use of each liquidity partner.

CRA-10.1.3B Licensees must submit on a quarterly basis, the following information within 10 business days from the end of the reporting period:

(a) A list of top 100 clients based on the total value traded during each month of the quarter. This report must include the following information:
  (i) Client ID;
  (ii) Place of residency;
  (iii) Crypto-asset type;
  (iv) Type of transaction (Buy or Sell);
  (v) Volume of transaction; and
  (vi) Value of transactions in USD;

(b) Particulars of any unexpected or unusual volatility, volumes and activity.

CRA-10.1 – Reporting Requirements (continued)

Annual License Fee

CRA-10.1.4 Licensees must complete and submit the Direct Debit Authorisation Form by 15th September and Form ALF (Annual License Fee) no later than 15th October to the CBB (ref. CRA-1.6.8 and CRA-1.6.9).

Institutional Information System (IIS)

CRA-10.1.5 Licensees are required to complete online non-financial information related to their institution by accessing the CBB's institutional information system (IIS). Licensees must update the required information at least on a quarterly basis or when a significant change occurs in the non-financial information included in the IIS. If no information has changed during the quarter, the licensee must still access the IIS quarterly and confirm the information contained in the IIS. Licensees must ensure that they access the IIS within 20 calendar days from the end of the related quarter and either confirm or update the information contained in the IIS.

CRA-10.1.6 [This Paragraph was deleted in XX 2023].

Reports Prepared by External Auditors

CRA-10.1.7 Licensees that hold or control client assets must arrange for their external auditor to perform an audit of client assets every 6 months on the licensees' compliance with the requirements related to the holding and segregation of the client's assets requirements. The report must be submitted to the CBB by 30th September for the 30th June report and 31st March for the 31st December report. The format of the Auditor's Report (Agreed Upon Procedure) is included in Part B of the Rulebook, as part of the supplementary information.

Onsite Inspection Reporting

CRA-10.1.8 For the purpose of onsite inspection by the CBB, licensees must submit requested documents and completed questionnaires to the Inspection Directorate at the CBB three working days ahead of inspection team entry date.

CRA-10.1 – Reporting Requirements (continued)

CRA-10.1.9 **Licensees must review the contents of the draft Inspection Report and submit to the Inspection Directorate at the CBB a written assessment of the observations/issues raised within fifteen working days of receipt of such report. Evidentiary documents supporting management's comments must also be included in the response package.**

CRA-10.1.10 **Licensees' board are required to review the contents of the Inspection Report and submit within one month, of the report issue date, a final response to such report along with an action plan addressing the issues raised within the stipulated timeline.**

CRA-10.1.11 [This Paragraph was deleted in XX 2023].

CRA-10.2 Notification Requirements

General Requirements

CRA-10.2.1 **All notifications and approvals required in this Module are to be submitted by licensees in writing.**

CRA-10.2.2 In this Module, the term 'in writing' includes electronic communication capable of being reproduced in paper form.

CRA-10.2.3 **Where a licensee is required to make notifications to the CBB or seek its approval under the requirements of this Rulebook, it must make the notification or seek approval immediately after it becomes aware of such a requirement.**

Matters Having a Serious Supervisory Impact

CRA-10.2.4 **Licensees must notify the CBB if any of the following has occurred, may have occurred or may occur in the near future:**

(a) The licensee failing to satisfy one or more of the requirements specified in this Module;

(b) Any matter which could have a significant adverse impact on the licensee's reputation;

(c) Any matter which could affect the licensee's ability to continue to provide adequate services to its customers and which could result in serious detriment to a customer of the licensee;

(d) Any matter in respect of the licensee that could result in material financial consequences to the financial system or to other licensees;

(e) A significant breach of any provision of the Rulebook;

(f) A breach of any requirement imposed by the relevant law or by regulations or an order made under any relevant law by the CBB; or

(g) If a licensee becomes aware, or has information that reasonably suggests that it has or may have provided the CBB with information that was or may have been false, misleading, incomplete or inaccurate, or has or may have changed in a material way. Such notification must be immediately made to the CBB.

CRA-10.2 Notification Requirements (continued)

CRA-10.2.5 The circumstances that may give rise to any of the events in Paragraph CRA-10.2.5 are wide-ranging and the probability of any matter resulting in such an outcome, and the severity of the outcome, may be difficult to determine. However, the CBB expects licensees to consider properly all potential consequences of events.

CRA-10.2.6 In determining whether an event that may occur in the near future should be notified to the CBB, a licensee should consider both the probability of the event happening and the severity of the outcome should it happen. Matters having a supervisory impact could also include matters relating to a controller that may indirectly have an effect on the licensee.

Legal, Professional, Administrative or other Proceedings Against a Licensee

CRA-10.2.7 **Licensees must notify the CBB immediately of any legal, professional or administrative or other proceedings instituted against it or its substantial shareholder that is known to the licensee and is significant in relation to the licensee's financial resources or its reputation.**

CRA-10.2.8 **Licensees must notify the CBB of the bringing of a prosecution for, or conviction of, any offence under any relevant law against the licensee that would prevent the licensee from undertaking its activities in fair, orderly and transparent manner or any of its Directors, officers or approved persons from meeting the fit and proper requirements of Section CRA-1.7.**

Fraud, Errors and other Irregularities

CRA-10.2.9 **Licensees must notify the CBB immediately if one of the following events arises:**

(a) It becomes aware that an employee may have committed fraud against one of its clients;

(b) It becomes aware that a person, whether or not employed by it, is acting with intent to commit fraud against it;

(c) It identifies irregularities in its accounting or other records, whether or not there is evidence of fraud;

(d) It suspects that one of its employees may be guilty of serious misconduct concerning his honesty or integrity and which is connected with the licensee's regulated activities; or

(e) Any conflicts of interest.

CRA-10.2 Notification Requirements (continued)

Insolvency, Bankruptcy and Winding Up

CRA-10.2.10 A licensee must notify the CBB immediately of any of the following events:

(a) The calling of a meeting to consider a resolution for winding up the licensee or a substantial shareholder of the licensee;

(b) An application to dissolve a substantial shareholder of the licensee or to strike the licensee off the Register of crypto-asset licensee;

(c) The presentation of a petition for the winding up of a substantial shareholder of the licensee;

(d) The making of any proposals, or the making of, a composition or arrangement with any one or more of the licensee's creditors, for material amounts of debt;

(e) An application for the appointment of an administrator or trustee in bankruptcy to a substantial shareholder of the licensee;

(f) The appointment of a receiver for a substantial shareholder of the licensee (whether an administrative receiver or a receiver appointed over particular property); or

(g) An application for an interim in relation to a substantial shareholder of the licensee under the applicable Bankruptcy laws.

External Auditor

CRA-10.2.11 Licensees must notify the CBB of the following:

(a) Removal or resignation of its external auditor; or

(b) Change in audit partner.

Approved Persons

CRA-10.2.12 [This Paragraph was deleted in XX 2023].

CRA-10.2.13 [This Paragraph was deleted in XX 2023].

CRA-10.2.14 [This Paragraph was deleted in XX 2023].

CRA-10.2.15 [This Paragraph was deleted in XX 2023].

CRA-10.3 Approval Requirements

Change in Name

CRA-10.3.1 Licensees must obtain CBB's prior written approval for any change in their legal name. Licensees must notify the CBB of any change in their corporate name at least one week prior to effecting the proposed change.

CRA-10.3.2 The request to change the licensee legal name must include the details of the proposed new name and the date on which the licensee intends to implement the change of name.

Change of Address

CRA-10.3.3 As specified in Article 51 of the CBB Law, a licensee must seek prior written approval from the CBB of a change in the address of the licensee's principal place of business in Bahrain, and that of its branches, if any.

CRA-10.3.4 The request under Paragraph CRA-10.3.3 must include the details of the proposed new address and the date on which the licensee intends to implement the change of address.

CRA-10.3.5 As specified in Article 51 of the CBB Law, a licensee must seek prior written approval from the CBB where it intends to carry on its business from new premises in Bahrain. This requirement applies whether or not the premises are to be used for the purposes of transacting business with clients, administration of the business or as the head office in Bahrain of the licensee.

Change in Legal Status

CRA-10.3.6 A licensee must seek the CBB's prior written approval in relation to any change in its legal status that may, in any way, affect its relationship with or limit its liability to its clients.

CRA-10.3 Approval Requirements (continued)

Change in Authorised or Issued Capital

CRA-10.3.7 As specified in Article 57(a) of the CBB Law, a licensee must seek the CBB's prior written approval before making any modification to its authorised or issued capital. In the case that a licensee has been granted approval to increase its paid-up capital, confirmation from the external auditor stating that the amount has been deposited in the licensee's bank account or otherwise reflected in the licensee's accounts will subsequently be required.

Client Asset Transfers

CRA-10.3.8 Licensees must seek prior written approval from the CBB before transferring client assets to a third party, in circumstances other than when acting on instructions from the client concerned.

Licensed Regulated Activities

CRA-10.3.9 Licensees wishing to cancel their license must obtain the CBB's written approval, before ceasing their activities. All such requests must be made in writing to the Director, Capital Markets Supervision, setting out in full the reasons for the request and how the business is to be wound up.

CRA-10.3.10 As specified in Article 50 of the CBB Law, a licensee wishing to cease to provide all or any of its licensed regulated crypto-asset services must obtain prior written approval from the CBB.

CRA-10.3.11 Licensees seeking to obtain the CBB's permission to cease business must submit to the CBB a formal request for the appointment of a liquidator acceptable to the CBB.

Carrying out Business in Another Jurisdiction

CRA-10.3.12 As specified in Article 51 of the CBB Law, a licensee must seek the CBB's prior written approval where it intends to undertake business activities in a jurisdiction other than Bahrain. The request for CBB approval must be made at least three months prior to planned commencement date of such business.

10.3 Approval Requirements (continued)

CRA-10.3.13 **Paragraph CRA-10.3.12 applies whether or not the licensee is required to be regulated locally in the jurisdiction where it proposes to undertake the business.**

CRA-10.3.14 The CBB will use the information to consider whether or not it should impose additional requirements on the licensee.

Mergers, Acquisitions, Disposals and Establishment of New Subsidiaries

CRA-10.3.15 **As specified in Articles 51 and 57 of the CBB Law, a licensee incorporated in Bahrain must seek prior written approval of the CBB where it intends to:**

(a) Enter into a merger with another undertaking;

(b) Enter into a proposed acquisition, disposal or establishment of a new subsidiary undertaking; or

(c) Open a new place of business as a subsidiary undertaking, a branch or a representative office within the Kingdom of Bahrain or other jurisdiction.

CRA-10.3.16 **Licensees wishing cease operation of a subsidiary must obtain the CBB's written approval, before ceasing the activities of the subsidiary.**

Outsourcing Arrangements

CRA-10.3.17 **[This Paragraph was deleted in XX 2023].**

CRA-10.3 Approval Requirements

Matters Having a Supervisory Impact

CRA-10.3.18 A licensee must seek prior approval from the CBB for any material changes or proposed changes to the information provided to the CBB in support of an authorisation application that occurs after authorisation has been granted.

CRA-10.3.19 Any licensee that wishes, intends or has been requested to do anything that might contravene, in its reasonable opinion, the provisions of UNSCR 1373 (and in particular Article 1, Paragraphs c) and d) of UNSCR 1373) must seek, in writing, the prior written opinion of the CBB on the matter (ref. AML-9.2.4).

CRA-10.3.20 As specified in Article 57 of the CBB Law, a licensee wishing to modify its Memorandum or Articles of Association, must obtain prior written approval of the CBB.

CRA-10.3.21 As specified in Article 57 of the CBB Law, a licensee wishing to transfer all or a major part of its assets or liabilities inside or outside the Kingdom, must obtain prior written approval from the CBB.

CRA-10.3.22 [This Paragraph was deleted in XX 2023].

CRA-10.3.23 [This Paragraph was deleted in XX 2023].

CRA-10.3.24 [This Paragraph was deleted in XX 2023].

CRA-10.3.25 [This Paragraph was deleted in XX 2023].

CRA-10.3.26 [This Paragraph was deleted in XX 2023].

Withdrawals

CRA-10.3.27 No funds may be withdrawn by shareholders from the licensee without the necessary prior written approval of the CBB.

CRA-11.1 Power to Request Information

CRA-11.1.1 **Licensees must provide all information that the CBB requests in order to discharge its regulatory obligations.**

CRA-11.1.2 **Licensees must provide all relevant information and assistance to the CBB inspectors and appointed experts on demand as required by Articles 111 and 114 of the CBB Law. Failure by licensees to cooperate fully with the CBB's inspectors or appointed experts, or to respond to their examination reports within the time limits specified, will be treated as demonstrating a material lack of cooperation with the CBB which will result in other enforcement measures.**

CRA-11.1.3 Article 163 of the CBB Law provides for criminal sanctions where false or misleading statements are made to the CBB or any person /appointed expert appointed by the CBB to conduct an inspection or investigation on the business of the licensee.

CRA-11.1.4 [This Paragraph was deleted in XX 2023]

CRA-11.2 Access to Premises

CRA-11.2.1 Representatives of the CBB, or persons appointed by the CBB may access, with or without notice, any of the licensee's business premises in relation to the discharge of the CBB's functions pursuant to the CBB Law.

CRA-11.2.2 **A licensee must take reasonable steps to ensure that its agents and providers under outsourcing arrangements permit such access to their business premises, to the CBB.**

CRA-11.2.3 **A licensee must take reasonable steps to ensure that each of its providers under material outsourcing arrangements deals in an open and cooperative way with the CBB in the discharge of its functions in relation to the licensee.**

CRA-11.2.4 The cooperation that licensees are expected to procure from such providers is similar to that expected of licensees themselves.

CRA-11.3 Accuracy of Information

CRA-11.3.1 A licensee must ensure that all information it provides to the CBB is:

(a) Factually accurate or, in the case of estimates and judgements, fairly and properly based on appropriate analysis and enquiries have been made by the licensee; and

(b) Complete, in that it should include everything which the CBB would reasonably and ordinarily expect to have or require.

CRA-11.3.2 If a licensee becomes aware, or has information that reasonably suggests that it has or may have provided the CBB with information that was or may have been false, misleading, incomplete or inaccurate, or has or may have changed in a material way, it must notify the CBB immediately. The notification must include:

(a) Details of the information which is or may be false, misleading, incomplete or inaccurate, or has or may have changed;

(b) An explanation why such information was or may have been provided in false, misleading, incomplete or inaccurate manner; and

(c) The correct information.

CRA-11.3.3 If the information in Paragraph CRA-11.3.2 cannot be submitted with the notification (because it is not immediately available), it must instead be submitted as soon as possible afterwards.

CRA-11.4 Methods of Information Gathering

CRA-11.4.1 The CBB uses various methods of information gathering on its own initiative which require the cooperation of licensees:

(a) Representatives of the CBB may make onsite visits at the premises of the licensee. These visits may be made on a regular basis, or on a sample basis, for special purposes such as theme visits (looking at a particular issue across a range of licensees), or when the CBB has a particular reason for visiting a licensee;

(b) Appointees of the CBB may also make onsite visits at the premises of the licensee. Appointees of the CBB may include persons who are not CBB staff, but who have been appointed to undertake particular monitoring activities for the CBB, such as in the case of Appointed Experts (refer to Section CRA-11.5).

(c) The CBB may request the licensee to attend meetings at the CBB's premises or elsewhere;

(d) The CBB may seek information or request documents by telephone, at meetings or in writing, including electronic communication;

(e) The CBB may require licensees to submit various documents or notifications, as per Chapter CRA-11, in the ordinary course of their business such as financial reports or upon the occurrence of a particular event in relation to the licensee such as a change in control.

CRA-11.4.2 When seeking meetings with a licensee or access to the licensee's premises, the CBB or the CBB appointee will access ~~to~~ a licensee's documents and personnel. Such requests will normally be made during reasonable business hours and with proper notice. However, there may be instances where the CBB may access the licensee's premises without prior notice.

CRA-11.4.3 The CBB expects that a licensee should:

(a) Make itself readily available for meetings with representatives or appointees of the CBB;

(b) Give representatives or appointees of the CBB reasonable access to any records, files, tapes or computer systems, which are within the licensee's possession or control, and provide any facilities which the representatives or appointees may reasonably request;

(c) Produce to representatives or appointees of the CBB specified documents, files, tapes, computer data or other material in the licensee's possession or control as as requested or required;

(d) Print information in the licensee's possession or control which is held on computer or otherwise convert it into a readily legible document or any other record which the CBB may reasonably request;

(e) Arrange for representatives or appointees of the CBB to copy documents of other material on the premises of the licensee at the licensee's expense and to remove copies and hold them elsewhere, or provide any copies, as requested by the CBB or its appointees; and

CRA-11.4 Methods of Information Gathering (continued)

(f) Answer truthfully, fully and promptly all questions which representatives or appointees of the CBB put to it.

CRA-11.4.4 The CBB considers that a licensee should ensure that the following persons act in the manner set out in Paragraph CRA-11.4.3:
(a) Its employees; and
(b) Any other members of its group and their employees.

CRA-11.4.5 [This Paragraph was deleted in XX 2023].

CRA-11.5 The Role of the Appointed Expert

Introduction

CRA-11.5.1 **The content of this Section is applicable to all licensees and appointed experts.**

CRA-11.5.2 The purpose of the contents of this Section is to highlight the roles and responsibilities of appointed experts when appointed pursuant to Article 114 or 121 of the CBB Law.

CRA-11.5.3 The CBB uses its own inspectors to undertake on-site examinations of licensees as an integral part of its regular supervisory role. In addition, the CBB may commission reports on matters relating to the business of licensees in order to assist it in assessing their compliance with CBB requirements.

CRA-11.5.4 [This Paragraph was deleted in XX 2023].

CRA-11.5.5 **Appointed experts must not be the same firm appointed as external auditor of the licensee.**

CRA-11.5.6 The CBB will decide on the range, scope and frequency of work to be carried out by appointed experts.

CRA-11.5.7 The appointment will be made in writing, and made directly with the appointed experts concerned. A separate letter is sent to the licensee, notifying them of the appointment. At the CBB's discretion, a trilateral meeting may be held at any point, involving the CBB and representatives of the licensee and the appointed experts, to discuss any aspect of the of the inspection or investigation or the report produced by the appointed expert.

CRA-11.5 The Role of the Appointed Expert (continued)

CRA-11.5.8 Following the completion of the investigation, the CBB will normally provide feedback on the findings of the investigation to the licensee.

CRA-11.5.9 Appointed experts will report directly to and be responsible to the CBB in this context and will specify in their report any limitations placed on them in completing their work (for example due to the licensee's group structure). The report produced by the appointed experts is the property of the CBB

CRA-11.5.10 **Compliance by appointed experts with the contents of this Chapter will not, of itself, constitute a breach of any other duty owed by them to a particular licensee (i.e. create a conflict of interest).**

CRA-11.5.11 The CBB may appoint one or more of its officials to work on the appointed experts' team for a particular licensee.

The Required Report

CRA-11.5.12 The scope of the required report will be determined and detailed by the CBB in the appointment letter. Appointed experts would normally be required to report on one or more of the following aspects of a licensee's business:
(a) Accounting and other records;
(b) Internal control systems;
(c) Returns of information provided to the CBB;
(d) Operations of certain departments; and/or
(e) Other matters specified by the CBB.

CRA-11.5.13 Appointed experts will be required to form an opinion on whether, during the period examined, the licensee is in compliance with the relevant provisions of the CBB Law and the CBB's relevant requirements, as well as other requirements of Bahrain Law and, where relevant, industry best practice locally and/or internationally.

CRA-11.5.14 **[This Paragraph was deleted in XX 2023].**

CRA-11.5 The Role of the Appointed Expert (continued)

CRA-11.5.15 **[This Paragraph was deleted in XX 2023].**

CRA-11.5.16 **[This Paragraph was deleted in XX 2023].**

CRA-11.5.17 **[This Paragraph was deleted in XX 2023].**

Other Notifications to the CBB

CRA-11.5.18 **Appointed experts must communicate to the CBB, during the conduct of their duties, any reasonable belief or concern they may have that any of the requirements of the CBB, including the licensing conditions are not or have not been fulfilled, or that there has been a material loss or there exists a significant risk of material loss in the concerned licensee, or that the interests of customers are at risk because of adverse changes in the financial position or in the management or other resources of the licensee. Notwithstanding the above, it is primarily the licensee's responsibility to report such matters to the CBB.**

CRA-11.5.19 [This Paragraph was deleted in XX 2023].

CRA-11.5 The Role of the Appointed Expert (continued)

CRA-11.5.20 [This Paragraph was deleted in XX 2023].

Permitted Disclosure by the CBB

CRA-11.5.21 **Appointed experts must keep all information relating to the licensee confidential and not divulge it to a third party except with the CBB's written permission or unless required by applicable laws in the Kingdom of Bahrain.**

CRA-11.5.22 [This Paragraph was deleted in XX 2023].

CRA-12.1 General Scope and Application

CRA-12.1.1 This Section sets out the Conduct of Business Obligations which licensees must adhere to.

CRA-12.1.2 This Section shall apply to all licensees offering regulated crypto-asset services except for Section CRA-12.5 which shall apply solely to licensees executing clients' orders.

CRA-12.2 Conflicts of interest

General Obligations

CRA-12.2.1 Licensees must adopt appropriate and transparent reporting lines within its organisation in order to ensure that issues involving risks of non-compliance with conflicts of interest Rules are given the necessary priority.

CRA-12.2.2 Licensees must establish, implement and maintain effective organisational and administrative arrangements appropriate to the size of the licensee and the nature, scale and complexity of its business, to prevent conflicts of interest from adversely affecting the interests of its clients.

CRA-12.2.3 The circumstances which should be treated as giving rise to a conflict of interest should cover cases where there is a conflict between the interests of the licensee or certain persons connected to the licensee or the group of which the licensee forms part, or from the performance of services and activities, and the duty the licensee owes to a client; or between the differing interests of two or more of its clients, to whom the licensee owes in each case a duty.

CRA-12.2.4 Licensees must establish, implement and maintain an effective conflicts of interest policy set out in writing and which is appropriate to the size of the licensee and the nature, scale and complexity of its business, to prevent conflicts of interest from adversely affecting the interests of its clients. The conflicts of interest policy must, at a minimum, include the following:

(a) The identification of, with reference to the specific services and activities carried out by or on behalf of the licensee, the circumstances which constitute or may give rise to a conflict of interest entailing a risk of damage to the interests of one or more clients;

(b) Procedures to be followed and measures to be adopted in order to manage such conflicts and to prevent such conflicts from damaging the interests of clients.

CRA-12.2.5 Licensees must assess and periodically review, at least annually, the conflicts of interest policy established and must take all appropriate measures to address any deficiencies.

CRA-12.2.6 [This Paragraph was deleted in XX 2023].

CRA-12.2 Conflicts of interest (Continued…)

CRA-12.2.7 Licensees must keep and regularly update a record of the situations or service carried out by or on behalf of the licensee in which a conflict of interest entailing a risk of damage to the interests of one or more clients has arisen or, in the case of an ongoing regulated crypto-asset service, may arise. Senior Management must receive on a periodic basis, and at least annually, written reports on situations referred to in this Rule.

Operational Independence

CRA-12.2.8 Licensees must take all appropriate steps to identify, and to prevent or manage conflicts of interest between the licensee, including their managers, employees, or any person directly or indirectly linked to them by control and their clients or between the interests of one client and another, including those caused by the receipt of inducements from third parties or by a licensee's own remuneration and other incentive structures.

CRA-12.2.9 The Board of Directors of a licensee must define, oversee and be accountable for the implementation of governance arrangements that ensure effective and prudent management of the licensee including the segregation of duties within that licensee and the prevention of conflicts of interest, and in a manner that promotes the integrity of the market and the interest of clients.

Remuneration Policy

CRA-12.2.10 Licensees must define and implement remuneration policies and practices under appropriate internal procedures taking into account the interests of all its clients. The remuneration policy must be approved by the Board of Directors of the licensee and be periodically reviewed, at least annually.

CRA-12.2.11 In defining its remuneration policies, a licensee must ensure that:

(a) Clients are treated fairly and their interests are not impaired by the remuneration practices adopted by the licensee in the short, medium or long term; and

(b) Remuneration policies and practices do not create a conflict of interest or incentive that may lead relevant persons to favour their own interests or the licensee's interest to the potential detriment of its clients.

CRA-12.2 Conflicts of interest (Continued)

Inducements Rules

CRA-12.2.12 Licensees providing its clients with advice on an independent basis or portfolio management must not accept and retain fees, for itself, commissions or any monetary or non-monetary benefits paid or provided by any third party or a person acting on behalf of a third party in relation to the provision of the services to clients. All fees, commissions or monetary benefits received from third parties in relation to the provision of advice on an independent basis and portfolio management must be transferred in full to the client.

Where the licensee receives minor non-monetary benefits that are capable of enhancing the quality of service provided to a client and are of a scale and nature such that they would not be deemed to impair compliance with the licensee's duty to act in the best interest of the client must be clearly disclosed and be excluded from the application of this Rule.

CRA-12.2.13 Licensees must set up and implement a policy to ensure that any fees, commissions or any monetary or non-monetary benefits paid or provided by any third party or a person acting on behalf of a third party in relation to the provision of advice on an independent basis and portfolio management are allocated and transferred to each individual client.

CRA-12.2.14 Licensees must inform clients about the fees, commissions or any monetary or non-monetary benefits transferred to them, such as through the periodic reporting statements provided to the client.

CRA-12.2.15 The Board of Directors must adopt and at least annually review the general principles of the inducements policy, and must be responsible for, and oversee, its implementation. The Board of Directors must also ensure that the compliance officer is involved in the establishment and the subsequent reviews of the inducements policy.

CRA-12.2.16 Licensees must not receive any remuneration, discount or non-monetary benefit for routing client orders to a particular trading venue which would infringe the requirements on conflicts of interest or inducements.

CRA-12.2 Conflicts of interest (Continued)

Personal Transaction

CRA-12.2.17 **Licensees must establish, implement and maintain adequate arrangements which prevent any relevant person who is involved in activities that may give rise to a conflict of interest, or who has access to inside information or to other confidential information relating to clients or transactions with or for clients by virtue of an activity carried out by him on behalf of the licensee.**

CRA-12.2.18 **Licensees must have a written policy governing employee dealing in crypto-assets, either through their own account or through related accounts, to eliminate, avoid, manage or disclose actual or potential conflicts of interests which may arise from such dealings.**

CRA-12.2.19 For the purposes of CRA-12.2.18, the term "related accounts" refers to accounts of the employee's spouse(s), children(s) of the employee or any other account(s) in which the employee holds any beneficial interest.

CRA-12.2.20 **The written policy governing employee's dealing in crypto-assets must specify the conditions under which an employee may deal in crypto-assets for their own account and related accounts (in particular, those who possess non-public information must be prohibited from dealing in the relevant crypto-assets). A copy of the policy must be provided to every employee at the time of joining as well as on periodic basis.**

CRA-12.2.21 **Transactions of employees' own account and related accounts must be actively monitored by the compliance officer and procedures to detect irregularities and ensure that the handling by the licensee of these transactions is not prejudicial to the interest of the licensee's other clients.**

CRA-12.2.22 **Any transactions for the employees own account and related accounts must be separately recorded and clearly identified in the records of the licensee.**

CRA-12.3 Sale Processes and Selling Practices

General Principles

CRA-12.3.1 Licensees must:

(a) Seek from its clients information relevant to the crypto-asset or regulated crypto-asset service requested;

(b) In the completion of any document, make it clear that all the answers or statements regarding the client's personal details and circumstances are the client's own responsibility. The client should always be required to assume responsibility for the completed document and be advised that incomplete and/or inaccurate information may prejudice the client's rights;

(c) Not withhold from the client any written evidence or documentation relating to the crypto-asset or regulated crypto-asset service without adequate and justifiable reasons being disclosed in writing and without delay to the client;

(d) Not recklessly, negligently or deliberately mislead a client in relation to the real or perceived advantages or disadvantages of any crypto-asset or regulated crypto-asset service;

(e) Ensure that all instructions from, or on behalf, of a client are processed properly and promptly;

(f) Have proper regard for the wishes of a client who seeks to terminate any agreement with it to carry out business;

(g) [This Subparagraph was deleted in XX 2023].

(h) Not exert undue pressure or undue influence on a client;

(i) Give advice only on those crypto-assets or regulated crypto-asset services in which the licensee is knowledgeable and seek or recommend other specialist advice when necessary; and

(j) Treat all information supplied by the client with complete confidentiality.

(k) [This Subparagraph was deleted in XX 2023].

CRA-12.3 Sale Processes and Selling Practices (Continued)

CRA-12.3.2 [This Paragraph was deleted in XX 2023].

CRA-12.3.3 For the purposes of CRA-12.3.1(j), the requirement to maintain all client information confidential shall not apply to:

(a) The disclosure of client information for such purposes, or in such circumstances as the CBB; or

(b) [This Subparagraph was deleted in XX 2023].

(c) The disclosure of client information pursuant to any requirement imposed under any applicable law or court order in the Kingdom of Bahrain.

CRA-12.3.4 Where a licensee deals with a person who is acting for a client under a power of attorney, the licensee must:

(a) obtain a certified true copy of the power of attorney;

(b) ensure that the power of attorney allows the person to act on the client's behalf; and

(c) operate within the limitations set out in the power of attorney.

CRA-12.3.5 [This Paragraph was deleted in XX 2023].

CRA-12.3.6 [This Paragraph was deleted in XX 2023].

CRA-12.3.7 [This Paragraph was deleted in XX 2023].

CRA-12.3.8 [This Paragraph was deleted in XX 2023].

CRA-12.3.9 [This Paragraph was deleted in XX 2023].

CRA-12.3.10 [This Paragraph was deleted in XX 2023].

CRA-12.3 Sale Processes and Selling Practices (Continued)

CRA-12.3.11 **[This Paragraph was deleted in XX 2023].**

CRA-12.3.12 **[This Paragraph was deleted in XX 2023].**

CRA-12.3.13 **[This Paragraph was deleted in XX 2023].**

CRA-12.3.14 [This Paragraph was deleted in XX 2023].

CRA-12.3.15 **[This Paragraph was deleted in XX 2023].**

CRA-12.3.16 **[This Paragraph was deleted in XX 2023].**

CRA-12.3.17 **[This Paragraph was deleted in XX 2023].**

CRA-12.4. Accepting Client and Contractual Agreement with Client

Terms of Business

CRA-12.4.1 **Licensees must provide clients with their terms of business, setting out the basis on which the regulated crypto-asset services are to be conducted.**

CRA-12.4.2 **The terms of business in relation to providing regulated crypto-asset services to a client must take the form of a client agreement.**

CRA-12.4.3 **The terms of business must include the rights and obligations of parties to the agreement, as well as other terms relevant to the regulated crypto-asset services.**

CRA-12.4.5 An application form in relation to regulated crypto-asset services will be deemed to be a client agreement, provided the form includes the principal terms and conditions of the service, such that the client is provided sufficient information to allow him to understand the basis on which the service is to be conducted.

CRA-12.4.6 **The client agreement must be provided in good time prior to providing the regulated crypto-asset services, and it must set out or refer to, among other matters, the rights and obligations of the parties to the agreement, and the terms on which the service is to be conducted.**

CRA-12.4.7 For the purposes of Paragraph CRA-12.4.6, "good time" should be taken to mean sufficient time to enable the client to consider properly the service or on offer before he is bound.

Client Understanding and Acknowledgement

CRA-12.4.8 **Licensees must not enter into a client agreement unless they have taken reasonable care to ensure that their client has had a proper opportunity to consider the terms.**

CRA-12.4.9 **Licensees must obtain their client's consent to the terms of the client agreement as evidenced by a signature or an equivalent mechanism.**

CRA-12.4.10 **The client agreement must contain the signature of both parties to the agreement. A copy of the signed client agreement must be provided by the licensee to the client.**

CRA-12.4.11 **Licensees must keep records of client agreements and any documents referred to in the client agreement the entire period the agreement is in force. Upon termination of the agreement, for whatsoever reason, the client agreement must be retained for a period of at least 5 years from the date of closure of the client account.**

CRA-12.5 Execution of Clients' Orders

CRA-12.5.1 Licensees must take sufficient steps to obtain, when executing orders, the best possible result for its clients taking into account the best execution factors of price, costs, speed, likelihood of execution and settlement, size, nature or any other consideration relevant to the execution of the order.

CRA-12.5.2 Whenever there is a specific instruction from a client, the licensee must execute the order following the specific instruction. The licensee shall be deemed to have satisfied its obligations to take all reasonable steps to obtain the best possible result for a client to the extent that it executes an order or a specific aspect of the order following specific instructions from a client relating to the order or the specific aspect of the order.

Order Execution Policy

CRA-12.5.3 Licensees must establish and implement an order execution policy to allow it to obtain, for its client orders, the best possible result.

CRA-12.5.4 Licensees must ensure that the trading venue or entity it selects will enable it to obtain results for its clients that are at least as good as the results that it reasonably could expect from using alternative entities.

CRA-12.5.5 Licensees must provide appropriate information to their clients on their order execution policy. That information must explain clearly, in sufficient detail and in a way that can easily be understood by clients.

CRA-12.5.6 Licensees must notify clients of any material changes to its order execution arrangements or order execution policy.

Monitoring and Review

CRA-12.5.7 A licensee must review, at least on an annual basis, its order execution policy and order execution arrangements.

CRA-12.5.8 A licensee must demonstrate to its clients, at their request, that it has executed their orders in accordance with the licensee's order execution policy and it must also ensure that it is able to demonstrate to the CBB upon request that the licensee is in compliance with this Module.

CRA-12.5 Execution of Clients' Orders (Continued…)

Client Order Handling Rules

CRA-12.5.9 When carrying out client orders, a licensee must implement procedures and arrangements which provide for the prompt, fair and expeditious execution of client orders, relative to the trading interests of the licensee.

CRA-12.5.10 A licensee must not misuse information relating to pending client orders, and shall take all reasonable steps to prevent the misuse of such information by any of its relevant persons.

CRA-12.5.11 A licensee must not carry out a client order or a transaction for own account in aggregation with another client order unless the following conditions are met:

(a) It is unlikely that the aggregation of orders and transactions will work overall to the disadvantage of a client whose order is to be aggregated;

(b) It is disclosed to each client whose order is to be aggregated that the effect of aggregation may work to its disadvantage in relation to a particular order;

(c) An order allocation policy must be established and effectively implemented, provided for the fair allocation of aggregated orders and transactions, including how the volume and price of orders determines allocations and the treatment of partial executions.

CRA-12.5.12 Where a licensee has aggregated transactions for own account with one or more clients' orders, such licensee must not allocate the related trades in a way that is detrimental to a Client.

CRA-12.5.13 Where a licensee aggregates a client order, with a transaction for own account and the aggregated order is partially executed, the licensee must allocate the related trades to the client in priority to itself, except where the licensee is able to demonstrate on reasonable grounds that without the combination it would not have been able to carry out the order on such advantageous terms, or at all, in which event it may allocate the transaction for own account proportionally, in accordance with its order allocation policy.

Selection of Trading Venues by Licensees

CRA-12.5.14 Licensees must not structure or charge its commission in such a way as to discriminate unfairly between trading venues.

CRA-13.1 General Requirements

CRA-13.1.1 **[This Paragraph was deleted in XX 2023].**

CBB's Approach to Market Abuse and Manipulation

CRA-13.1.1A The risk of market abuse and manipulation, such as, but not limited to, price manipulation, inside trading, price rigging, non-disclosure of material information, disclosure of false or misleading information and other similar actions poses a significant challenge to establish fair, transparent and orderly market in crypto-assets.

CRA-13.1.1B **Licensees and issuers of digital tokens must comply with the same set of requirements contained in Module Prohibition of Market Abuse and Manipulation (Module MAM) including adherence to:**

(a) Accepted market practices;
(b) Prohibited conduct in possession of insider information;
(c) Prohibited market conduct; and
(d) Penalty for contravention

Policies for Prevention of Market Abuse and Manipulation

CRA-13.1.1C **Licensees must establish and implement written policies and controls for the proper surveillance of its trading platform in order to identify, prevent and report any manipulative or abusive trading activities. The policies and controls should, at a minimum, cover the following:**

(a) Preventing any potential market abuse or manipulation;
(b) monitoring activity on its platform;
(c) identifying anomalies; and
(d) taking immediate steps to restrict or suspend trading upon discovery of manipulative or abusive activities (for example, temporarily suspending accounts).

CRA-13.1.1D **A licensee must notify the CBB as soon as practicable of any market manipulative or abusive activities on its trading platform (whether potential, attempted or conducted). The licensee must provide the CBB with full assistance in connection with such activities and implement appropriate remedial measures.**

CRA-13.1 General Requirements (continued)

Market Surveillance System

CRA-13.1.1E **In addition to internal market surveillance policies and controls referred to in Paragraph CRA-13.1.1C above, a licensee must adopt an effective market surveillance system provided by a reputable and independent provider to identify, monitor, detect and prevent any market manipulative or abusive activities on its platform, and provide access to this system to the CBB to perform its own surveillance functions when required by the CBB.**

CRA-13.1.1F **A licensee must review the effectiveness of the market surveillance system provided by the independent provider on a regular basis, at least annually, and make enhancements as soon as practicable to ensure that market manipulative or abusive activities are properly identified. The review report should be submitted to the CBB upon request.**

CRA-13.1.2 **[This Paragraph was deleted in XX 2023].**

CRA-13.1.3 **[This Paragraph was deleted in XX 2023].**

CRA-13.1.4 [This Paragraph was deleted in XX 2023].

CRA-13.2 [This Section was deleted in XX 2023]

CRA-13.2.1 **[This Paragraph was deleted in XX 2023].**

CRA-13.2.2 [This Paragraph was deleted in XX 2023].

CRA-13.2.3 [This Paragraph was deleted in XX 2023].

CRA-13.2.4 **[This Paragraph was deleted in XX 2023].**

CRA-13.2.5 [This Paragraph was deleted in XX 2023].

CRA-13.2.6 [This Paragraph was deleted in XX 2023].

CRA-13.2.7 **[This Paragraph was deleted in XX 2023].**

CRA-13.2.8 **[This Paragraph was deleted in XX 2023].**

CRA-13.2.9 [This Paragraph was deleted in XX 2023].

CRA-13.2.10 **[This Paragraph was deleted in XX 2023].**

CRA-13.2.11 **[This Paragraph was deleted in XX 2023].**

CRA-13.2.12 **[This Paragraph was deleted in XX 2023].**

CRA-13.3 [This Section was deleted in XX 2023]

CRA-13.3.1	[This Paragraph was deleted in XX 2023].
CRA-13.3.2	[This Paragraph was deleted in XX 2023].
CRA-13.3.3	[This Paragraph was deleted in XX 2023].
CRA-13.3.4	[This Paragraph was deleted in XX 2023].

CRA-13.4 [This Section was deleted in XX 2023]

CRA-13.4.1	[This Paragraph was deleted in XX 2023].
CRA-13.4.2	[This Paragraph was deleted in XX 2023].
CRA-13.4.3	[This Paragraph was deleted in XX 2023].
CRA-13.4.4	[This Paragraph was deleted in XX 2023].
CRA-13.4.5	[This Paragraph was deleted in XX 2023].

CRA-13.5 [This Section was deleted in XX 2023]

CRA-13.5.1 **[This Paragraph was deleted in XX 2023].**

CRA-13.5.2 [This Paragraph was deleted in XX 2023].

CRA-13.5.3 **[This Paragraph was deleted in XX 2023].**

CRA-13.5.4 **[This Paragraph was deleted in XX 2023].**

CRA-13.6 [This Section was deleted in XX 2022]

CRA-13.6.1	[This Paragraph was deleted in XX 2023].
CRA-13.6.2	[This Paragraph was deleted in XX 2023].
CRA-13.6.3	[This Paragraph was deleted in XX 2023].

CRA-13.7 [This Section was deleted in XX 2023]

CRA-13.7.1	[This Paragraph was deleted in XX 2023].
CRA-13.7.2	[This Paragraph was deleted in XX 2023].

CRA-13.8 [This Section was deleted in XX 2023]

CRA-13.8.1 [This Paragraph was deleted in XX 2023].

CRA-13.9 [This Section was deleted in XX 2023]

CRA-13.9.1	[This Paragraph was deleted in XX 2023].
CRA-13.9.2	[This Paragraph was deleted in XX 2023].

MODULE	CRA:	Crypto-asset
CHAPTER	CRA-14	[This Chapter was deleted in XX 2023]

CRA-14.1 [This Section was deleted in XX 2023]

CRA-14.1.1 [This Paragraph was deleted in XX 2023].

CRA-14.1.2 [This Paragraph was deleted in XX 2023].

CRA-14.1.3 [This Paragraph was deleted in XX 2023].

CRA-14.1.4 [This Paragraph was deleted in XX 2023].

CRA-14.1.5 [This Paragraph was deleted in XX 2023].

CRA-14.1.6 [This Paragraph was deleted in XX 2023].

CRA-14.1.7 [This Paragraph was deleted in XX 2023].

CRA-14.1.8 [This Paragraph was deleted in XX 2023].

CRA-14.1.9 [This Paragraph was deleted in XX 2023].

CRA-14.1.10 [This Paragraph was deleted in XX 2023].

CRA-14.1.11 [This Paragraph was deleted in XX 2023].

CRA-14.1.12 [This Paragraph was deleted in XX 2023].

CRA-14.1.13 [This Paragraph was deleted in XX 2023].

CRA-14.1.14 [This Paragraph was deleted in XX 2023].

MODULE	CRA:	Crypto-asset
CHAPTER	CRA-14	[This Chapter was deleted in XX 2023]

CRA-14.2 [This Section was deleted in XX 2023]

CRA-14.2.1 [This Paragraph was deleted in XX 2023].

CRA-14.2.2 [This Paragraph was deleted in XX 2023].

CRA-14.2.3 [This Paragraph was deleted in XX 2023].

CRA-14.2.4 [This Paragraph was deleted in XX 2023].

CRA-14.2.5 [This Paragraph was deleted in XX 2023].

CRA-14.2.6 [This Paragraph was deleted in XX 2023].

MODULE	CRA:	Crypto-asset
CHAPTER	CRA-14	[This Chapter was deleted in XX 2023]

CRA-14.3 [This Section was deleted in XX 2023]

CRA-14.3.1 [This Paragraph was deleted in XX 2023].

CRA-14.3.2 [This Paragraph was deleted in XX 2023].

CRA-14.3.3 [This Paragraph was deleted in XX 2023].

CRA-14.3.4 [This Paragraph was deleted in XX 2023].

CRA-14.3.5 [This Paragraph was deleted in XX 2023].

CRA-14.3.6 [This Paragraph was deleted in XX 2023].

CRA-14.3.7 [This Paragraph was deleted in XX 2023].

CRA-14.4 [This Section was deleted in XX 2023]

CRA-14.4.1 [This Paragraph was deleted in XX 2023].

CRA-14.4.2 [This Paragraph was deleted in XX 2023].

CRA-14.4.3 [This Paragraph was deleted in XX 2023].

CRA-14.4.4 [This Paragraph was deleted in XX 2023].

CRA-14.4.5 [This Paragraph was deleted in XX 2023].

MODULE	CRA:	Crypto-asset
CHAPTER	CRA-14	[This Chapter was deleted in XX 2023]

CRA-14.5 [This Section was deleted in XX 2023]

CRA-14.5.1 [This Paragraph was deleted in XX 2023].

CRA-14.5.2 [This Paragraph was deleted in XX 2023].

CRA-14.5.3 **[This Paragraph was deleted in XX 2023].**

CRA-14.5.4 [This Paragraph was deleted in XX 2023].

CRA-14.5.6 [This Paragraph was deleted in XX 2023].

CRA-14.5.7 [This Paragraph was deleted in XX 2023].

CRA-14.5.8 [This Paragraph was deleted in XX 2023].

CRA-14.5.8 [This Paragraph was deleted in XX 2023].

CRA-14.5.9 [This Paragraph was deleted in XX 2023].

CRA-14.5.10 [This Paragraph was deleted in XX 2023].

MODULE	CRA:	Crypto-asset
CHAPTER	CRA-14	[This Chapter was deleted in XX 2023]

CRA-14.6 [This Section was deleted in XX 2023]

CRA-14.6.1 [This Paragraph was deleted in XX 2023].

CRA-14.6.2 [This Paragraph was deleted in XX 2023].

CRA-14.6.3 [This Paragraph was deleted in XX 2023].

CRA-14.6.4 [This Paragraph was deleted in XX 2023].

CRA-14.6.5 [This Paragraph was deleted in XX 2023].

CRA-14.6.6 [This Paragraph was deleted in XX 2023].

CRA-14.6.7 [This Paragraph was deleted in XX 2023].

CRA-14.6.8 [This Paragraph was deleted in XX 2023].

CRA-14.6.9 [This Paragraph was deleted in XX 2023].

CRA-14.6.10 [This Paragraph was deleted in XX 2023].

CRA-14.6.11 [This Paragraph was deleted in XX 2023].

CRA-14.6.12 [This Paragraph was deleted in XX 2023].

CRA-14.6.13 [This Paragraph was deleted in XX 2023].

CRA-14.6.14 [This Paragraph was deleted in XX 2023].

CRA-14.6.15 [This Paragraph was deleted in XX 2023].

CRA-14.6.16 [This Paragraph was deleted in XX 2023].

CRA-14.6.17 [This Paragraph was deleted in XX 2023].

CRA-14.6.18 [This Paragraph was deleted in XX 2023].

CRA-14.6.19 [This Paragraph was deleted in XX 2023].

CRA-14.6.20 [This Paragraph was deleted in XX 2023].

CRA-14.6.21 [This Paragraph was deleted in XX 2023].

CRA-14.6.22 [This Paragraph was deleted in XX 2023].

CRA-14.6.23 [This Paragraph was deleted in XX 2023].

MODULE	CRA:	Crypto-asset
CHAPTER	CRA-14	[This Chapter was deleted in XX 2023]

CRA-14.7 [This Section was deleted in XX 2023]

CRA-14.7.1 [This Paragraph was deleted in XX 2023].

CRA-14.7.2 [This Paragraph was deleted in XX 2023].

CRA-14.7.3 [This Paragraph was deleted in XX 2023].

CRA-14.7.4 [This Paragraph was deleted in XX 2023].

CRA-14.7.5 [This Paragraph was deleted in XX 2023].

CRA-14.7.6 [This Paragraph was deleted in XX 2023].

CRA-14.7.7 [This Paragraph was deleted in XX 2023].

CRA-14.7.8 [This Paragraph was deleted in XX 2023].

MODULE	CRA:	Crypto-asset
CHAPTER	CRA-14	[This Chapter was deleted in XX 2023]

CRA-14.8 [This Section was deleted in XX 2023]

CRA-14.8.1 [This Paragraph was deleted in XX 2023].

CRA-14.8.2 [This Paragraph was deleted in XX 2023].

CRA-14.8.3 [This Paragraph was deleted in XX 2023].

CRA-14.8.4 [This Paragraph was deleted in XX 2023].

CRA-14.8.5 [This Paragraph was deleted in XX 2023].

CRA-14.8.6 [This Paragraph was deleted in XX 2023].

CRA-14.8.7 [This Paragraph was deleted in XX 2023].

CRA-14.8.8 [This Paragraph was deleted in XX 2023].

CRA-14.8.9 [This Paragraph was deleted in XX 2023].

MODULE	CRA:	Crypto-asset
CHAPTER	CRA-14	[This Chapter was deleted in XX 2023]

CRA-14.9 [This Section was deleted in XX 2023]

CRA-14.9.1 [This Paragraph was deleted in XX 2023].

CRA-14.9.2 [This Paragraph was deleted in XX 2023].

CRA-14.9.3 [This Paragraph was deleted in XX 2023].

CRA-14.9.4 [This Paragraph was deleted in XX 2023].

CRA-14.9.5 [This Paragraph was deleted in XX 2023].

CRA-14.9.6 [This Paragraph was deleted in XX 2023].

CRA-14.9.7 [This Paragraph was deleted in XX 2023].

CRA-14.9.8 [This Paragraph was deleted in XX 2023].

CRA-14.9.9 [This Paragraph was deleted in XX 2023].

CRA-14.9.10 [This Paragraph was deleted in XX 2023].

MODULE	CRA:	Crypto-asset
CHAPTER	CRA-14	[This Chapter was deleted in XX 2023]

CRA-14.10 [This Section was deleted in XX 2023]

CRA-14.10.1 [This Paragraph was deleted in XX 2023].

CRA-14.10.2 [This Paragraph was deleted in XX 2023].

CRA-14.10.3 [This Paragraph was deleted in XX 2023].

CRA-14.10.4 [This Paragraph was deleted in XX 2023].

CRA-14.10.5 [This Paragraph was deleted in XX 2023].

CRA-14.10.6 [This Paragraph was deleted in XX 2023].

CRA-14.10.7 [This Paragraph was deleted in XX 2023].

CRA-14.10.8 [This Paragraph was deleted in XX 2023].

CRA-14.10.9 [This Paragraph was deleted in XX 2023].

CRA-14.10.10 [This Paragraph was deleted in XX 2023].

[Appendix -1 was deleted in XX 2023]

[Appendix -2 was deleted in XX 2023]

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.1 Digital Token Offerings

CRA-15.1.1 **A company must not make an offer or issue a digital token whose issuance is regulated by the CBB unless it has obtained a written approval from the CBB. Prior to offering a digital token, the digital token issuer must meet the eligibility criteria and requirements set out in this Module.**

Digital Tokens

CRA-15.1.2 **All offers of digital tokens which exhibit the characteristics of a security are regulated by the CBB.**

CRA-15.1.3 **While determining whether a digital token qualifies as a security, the CBB will examine the underlying economic purpose of the digital token, its structure and characteristics, including the rights attached to the digital token. For the avoidance of doubt, a digital token may be considered:**

(a) Equivalent of an equity security: where it confers or represents ownership interest in the issuer or gives entitlement to share in the issuer's profit; or

(b) Equivalent of a bond or debt security: where it constitutes or evidences the indebtedness of the issuer of the digital token in respect of any money that is lent to the issuer by the digital token holder, its maturity is fixed, is redeemable at maturity and gives entitlement to share in interest distributed by the digital token issuer.

CRA-15.1.4 In order to determine whether a digital token is considered a security, the CBB shall, amongst other things, take into consideration the following:

(a) Does it give the digital token holder an entitlement against the digital token issuer? If so, is the entitlement in kind or a monetary entitlement? If it is monetary entitlement, is it profit sharing, a predetermined entitlement, or an undetermined other kind of entitlement?

(b) Does the digital token represent a monetary claim on the digital token issuer?

(c) Is the digital token transferable?

(d) Does it confer decision power on the project of the digital token issuer?

CRA-15.1 Digital Token Offerings (continued)

CRA-15.1.5 The guidance provided are indicative and not exhaustive and, the CBB may take into consideration additional factors while assessing an application for issuance of a digital token. A digital token shall be considered a security if it is either a utility token or an asset token and exhibits the following characteristic:

(a) Utility tokens: A utility token shall be considered a security if it has an investment purpose at the point of issue or it has the potential to become investment objects. To this end, utility tokens which are transferable shall be considered as securities.
A utility token shall not be treated as a security if its sole purpose is to confer digital access rights to an application or a service, and if the utility token can actually be used in this way at the point of issue. In such cases, the underlying function is to grant access rights and the connection and resemblance to an equity security or debt security is absent.

(b) Asset tokens: An asset token shall be treated as a security where it:

(i) gives rights to financial entitlement and exhibits features of either bonds or equity securities: the former if the entitlement is a predetermined cash flow; and the latter if the entitlement is a share in profit;

(ii) gives right to an entitlement in kind, and the token holder holds decision making powers in the project.

Initial Assessment

CRA-15.1.6 Potential digital token issuers seeking to undertake a digital token offer are encouraged to initiate preliminary discussion with the CBB to determine whether the digital token is regulated by the CBB. As part of the initial assessment, potential digital token issuers should provide necessary details, including details about the issuer and description of the project, to the CBB to determine suitability of the digital token for issuance.

CBB's Right of Refusal or Restrictions on Digital Token Offering

CRA-15.1.7 The CBB may reject an application for offering of digital tokens if it is found that the issuance thereof might cause damage or be contrary to the interests of the holders of the digital tokens or the market in general.

CRA-15.1.8 Where the CBB grants its approval in relation to an offering, it may impose additional conditions, as it deems necessary.

CRA-15.1 Digital Token Offerings (continued)

General Requirements

CRA-15.1.9 The digital token issuer must meet the following requirements for a digital token offering:

(a) The digital token issuer must be a legal person duly incorporated under the laws of the Kingdom of Bahrain or a jurisdiction acceptable to the CBB and which is not publicly listed on a stock exchange;

(b) The digital token issuer must ensure no conflict of interest arises during the issuance of digital tokens;

(c) The digital token issuer must protect and act in the best interests of digital token holders as well as provide equal treatment to all digital token holders;

(d) The digital token issuer must adhere to the offering and issuing timetable contained in the whitepaper, or as amended, subject to the CBB's written approval;

(e) The maturity period of a digital token exhibiting characteristics of a debt security must not exceed 5 years;

(f) For any single offering of digital token, the digital tokens must have identical terms and conditions of issuance, including having the same price; and

(g) The offer period for a digital token offering must not be less than 10 calendar days after the day of commencement of the offer and must not exceed a maximum period of three (3) months.

CRA-15.1.10 The digital token issuer and the digital token advisor must fulfil all obligations in their respective capacities in accordance with the signed written agreements concluded between them in respect of the digital token issue.

CRA-15.1 Digital Token Offerings (continued)

Moratorium on Equity Interest

CRA-15.1.11 Founders and senior management of the digital token issuer must, in aggregate, own at least 50% equity holding in the digital token issuer, on the date of the issuance of the digital tokens.

CRA-15.1.12 Post issuance of the digital tokens, the founders and senior management of the digital token issuer are not entitled to sell or transfer their shareholding for a period of 1 year, starting from the date of the issuance of the digital tokens

Cooling-off Period

CRA-15.1.13 A cooling-off right must be given to an investor who is investing in a digital token offering, except for where such investor is a shareholder, board member or an employee of the digital token issuer. The cooling-off period must be not less than two (2) business days commencing from the date of close of the issue. No fee or penalty must be charged to the investor who exercises the right to a refund during the cooling-off period.

CRA-15.1.14 Investors exercising their cooling-off rights must be refunded within five (5) business days. The refund amount must be the sum of:

(a) The purchase price paid for the digital token; and

(b) Any other charges imposed at the time of purchase of the digital token.

Soft Cap (Minimum Subscription)

CRA-15.1.15 The soft cap must not be set lower than 80% of the digital token offer size. Digital token issuers may set a higher soft cap.

CRA-15.1 Digital Token Offerings (continued)

CRA-15.1.16 Where a digital token offer fails to reach the soft cap as set in the whitepaper, the digital token advisor must within five (5) business days from the closure of the digital token offering:

(a) Send each investor a notification about the failure to reach the soft cap and refund the subscription amount and other charges that the investor paid for the digital token offer; and

(b) Report the failure to reach the soft cap, the refund made and cancellation of the digital token offer to the CBB.

Oversubscription

CRA-15.1.17 If a digital token offering is over-subscribed after the closing of the offering period, the digital token advisor must make allotment in accordance with the pre-determined basis which must be described in the whitepaper. The digital token advisor must not make allotment in excess of the limit stated in the whitepaper and any excess subscription amounts received from investors must be refunded to investors within 3 business days from the date of allotment.

Release of Funds

CRA-15.1.18 The digital token issuer and the digital token advisor must enter into an agreement with provisions, among other matters, on the schedule of release of proceeds (if stated in the whitepaper), the progress report that will be required before each release of proceeds, and that the digital token advisor will return the said proceeds to the investors in case the soft cap of the digital token offer is not reached or in a pro-rata basis in case the project is not completed by the digital token issuer.

CRA-15.1.19 The banking arrangement for the purpose of managing subscription money between the digital token issuer and the digital token advisor must be dissolved upon completion of fund transfer process, unless the digital token offering failed to meet the soft cap target or the project is not completed by the digital token issuer with notification to the CBB.

CRA-15.1 Digital Token Offerings (continued)

CRA-15.1.20 If the digital token issuer is not able to complete the project, the appointed digital token advisor must:

(a) Immediately notify the CBB regarding the non-completion of the project by the digital token issuer and the reason behind the project not being completed; and

(b) Within 5 business days from the date of notifying the CBB, individually notify each investor about the non-completion of the project and refund the remaining proceeds under its care on a pro-rata basis to the investors based on the amount of their investment.

Allotment

CRA-15.1.21 Digital tokens must be allotted to subscribing investors within 6 calendar days of the closing date of the digital token offer in accordance with the allotment basis stipulated in the whitepaper. The subscription results must be announced on the digital token advisor's platform.

Approval Requirements

CRA-15.1.22 A digital token issuer must submit the application along with the draft whitepaper and other documents as specified in Paragraph CRA-15.1.28, through its digital token advisor, in a form and manner as specified by the CBB, including the liabilities of its signatories and a fit and proper declaration of its board members and senior management.

CRA-15.1.23 The digital token issuer must demonstrate to the CBB that the gross proceeds to be raised from the digital token offering would be sufficient to undertake the project or business as proposed in the whitepaper.

CRA-15.1.24 The CBB will make a decision on the application within 30 working days of receipt of all required information and documents complete in all respect.

CRA-15.1.25 The CBB's approval for an offer of digital tokens does not mean that it has approved the appropriateness of the digital token issuer's project or authenticated the financial and technical information presented in the whitepaper.

CRA-15.1 Digital Token Offerings (continued)

Suspension or Withdrawal of the Approval

CRA-15.1.26 **Notwithstanding the approval granted by the CBB to the digital token issuer, the CBB may, at any time during the offer period, or before the funds raised is released to the digital token issuer, do any or all of the following:**

(a) Revoke the CBB's approval;

(b) Issue a direction to suspend the digital token offering; or

(c) Issue a direction to defer the implementation of the digital token offering.

CRA-15.1.27 The CBB may exercise its powers under Paragraph CRA-15.1.26 if the CBB becomes aware of any of the following:

(a) The digital token issuer has breached the CBB Law, its regulations, resolutions or directives (including any requirement of this Module or any other applicable Modules of the CBB Rulebook);

(b) The digital token issuer has failed to comply with any terms or conditions imposed by the CBB and/or the digital token advisor;

(c) The application, including the whitepaper, contains any statement or information that is false or misleading or from which there is a material omission; or

(d) There is a concern with regards to the digital token issuer's corporate governance record or with the integrity of any of the digital token issuer's directors and senior management.

Documentation Requirements

CRA-15.1.28 **A digital token issuer, through its appointed digital token advisor, must provide the CBB the following documents:**

(a) A draft whitepaper prepared in accordance with the requirements of this Module;

(b) An up-to-date copy of the memorandum and articles of association;

(c) A copy of the digital token issuer's Board of Directors' resolution approving the issuance of digital tokens;

(d) Copies of audited financial statements. A company that has been established for less than one year must submit projected financial statements whereas a company that has been established for a longer period (more than 1 year) must provide the financial statements for the past financial years going up to a maximum of preceding 3 financial years;

CRA-15.1 Digital Token Offerings (continued)

(e) Documents proving the establishment of an arrangement that ensures the monitoring and safeguarding of the funds to be collected through the digital token offering in accordance with Paragraph CRA-15.2.10;
(f) A copy of the agreement entered into with the appointed licensed retail bank for deposit of funds to be raised through the digital token offer;
(h) All proposed marketing material related to the digital token offering;
(i) A declaration by the digital token advisor confirming its responsibility for carrying out due diligence on the digital token issuer and assessing accuracy of the information contained in the whitepaper and other documents submitted as part of the application (Appendix CRA-2);
(j) A declaration by the Board of Directors regarding the reliability and accuracy of the information provided to the CBB as part of the digital token offering requirements (Appendix CRA-3);
(k) A copy of the duly signed declaration by the legal advisor for the digital token offer, based on a due diligence exercise of all applicable laws, facts and arrangements, including enforceability of the rights relating to the digital tokens, as appropriate (Appendix CRA-4); and
(l) Any other information as required by the CBB.

Registration of Whitepaper

CRA-15.1.29 The final corrected copies of the whitepaper and other documents must be registered with the CBB no later than 2 business days prior to the date of commencement of the offering period.

CRA-15.1 Digital Token Offerings (continued)

Contents of the Whitepaper

CRA-15.1.30 The whitepaper must contain, in both the Arabic and English language, all the information concerning the digital token issuer and the proposed digital token offering that would enable investors to make an informed investment decision and understand the risks relating to the offering. The information in the whitepaper must, at a minimum, include the following:

(a) A detailed description of the digital token issuer's project, the reasons for the offering and the planned use of the funds raised;

(b) Detailed information about the directors, senior management, key personnel and advisers involved in the project's design and development including the name, designation, nationality, address, professional qualifications and related experience;

(c) The business plan of the digital token issuer;

(d) The key characteristics of the digital token including the rights, conditions, function and obligations attached to the digital tokens including any specific rights attributed to a token holder and the procedures and conditions of exercise of these rights;

(e) A summary of the legal opinion regarding the priority of the claims of digital token holders in the event of insolvency or liquidation of the digital token issuer;

(f) A detailed description of the digital token offering, including but not limited to:

(g) The number of digital tokens to be issued;

(h) The digital token issue price;

(i) The subscription terms and conditions;

(j) The minimum amount necessary to carry out the project and the maximum amount of the offering; and

(k) The subsequent use and application of the proceeds thereafter illustrated in a scheduled timeline for drawdown and utilisation of proceeds ("schedule of proceeds");

(l) The technical specifications of the digital token;

(m) The risks relating to the digital token issuer, the digital tokens, the digital token offering and the carrying out of the project, as well as mitigating measures thereof;

CRA-15.1 Digital Token Offerings (continued)

(n) A detailed description on the determination of the accounting and the valuation treatments for the digital tokens including all valuation methodology and reasonable presumptions adopted in such calculation;

(o) The allotment policy for the digital tokens;

(p) A detailed technical description of the protocol, platform and/or application of the digital token, as the case may be, and the associated benefits of the technology;

(e) Detailed description of the sustainability and scalability of the underlying business or project;

(f) Detailed description of the financial, technical, legal and commercial due diligence and market feasibility undertaken on the project;

(g) Financial statements of the digital token issuer in accordance with CRA15.1.28(d); and

(h) The offering timetable.

CRA-15.1.31 The whitepaper must not include presentation of estimates, projections, forecasts, or forward-looking statements, or overviews, without sufficient qualification, or without sufficient factual basis and reasonable assumptions.

CRA-15.1.32 The information provided in the whitepaper must be fair, clear, accurate, complete in all respects and not misleading, and must be presented in a concise and comprehensible manner. It must not include any promotional statements to excite rather than to inform.

CRA-15.1.33 The whitepaper must be prepared in accordance with the template provided in Appendix CRA-1.

CRA-15.1.34 The CBB, prior to approving an application for offering of digital tokens, shall assess whether the information provided in the whitepaper is complete and comprehensible. The whitepaper should be drawn up by the digital token issuer under the guidance of the digital token advisor prior to being submitted to the CBB.

CRA-15.1.35 Along with the whitepaper, a summary of the whitepaper must be made available to investors both in the Arabic and English language.

CRA-15.1 Digital Token Offerings (continued)

CRA-15.1.36 The digital token issuer must describe in the whitepaper the procedures for collection and management of the funds raised through the digital token offering. The digital token issuer must ensure the consistency of these procedures relative to the duration of the offering and the planned use of the funds collected.

CRA-15.1.37 The mechanism for collection of funds must offer sufficient guarantees ensuring its reliability and efficiency. It must have at least the following characteristics:

(a) It must ensure the security of the funds collected;

(b) It must ensure that the funds collected are deposited in a CBB licensed retail bank account in Bahrain dedicated specifically to the digital token offering;

(c) It must ensure that the funds collected cannot be transferred to the digital token issuer unless the soft cap threshold is reached; and

(d) It must ensure that the funds collected can be transferred to the digital token issuer or used by the digital token issuer only if the drawdown conditions provided for by the digital token issuer in the whitepaper are met.

Responsibility for Reliability and Accuracy of the Whitepaper

CRA-15.1.38 The whitepaper and the supplementary whitepaper must include a duly signed Board of Directors responsibility statement. The signature on the whitepaper and the supplementary whitepaper by the Board of Directors must be preceded by a declaration specifying that, to their knowledge, the information presented in the whitepaper corresponds to the facts, there is no omission liable to make it misleading and that they accept full responsibility for the information contained in the whitepaper.

Validity of the Whitepaper Approval by the CBB

CRA-15.1.39 The whitepaper remains valid for a maximum period of six months from the date of notification of the CBB's approval. After this period, no person shall offer digital tokens based on such whitepaper, unless approved by the CBB.

CRA-15.1 Digital Token Offerings (continued)

Supplementary Whitepaper

CRA-15.1.40 Where a digital token issuer or digital token advisor becomes aware of new facts which have a significant influence on the investment decision, after the whitepaper has been approved by the CBB, but before the closing of the offer period, the digital token issuer must immediately notify the CBB and furnish a supplementary whitepaper to the CBB. At a minimum, a supplementary whitepaper must be filed with the CBB, upon occurrence of the following:

(a) A matter has arisen, and information in respect of that matter would have required by these Rules to be disclosed in the whitepaper if the matter had arisen at the time the whitepaper was prepared;

(b) There has been a material change affecting a matter disclosed in the whitepaper;

(c) The whitepaper contains a statement or information that is false or misleading;

(d) The whitepaper contains a statement or information from which there is a material omission; or

(e) Where the assumptions based upon which the project or business proposition, the due diligence, or market feasibility were made are no longer valid or reliable.

CRA-15.1.41 Where a digital token issuer files a supplementary whitepaper with the CBB, it must immediately inform investors about the filing of a supplementary whitepaper by announcing it on the digital token advisor's platform, as well as on its own website.

CRA-15.1.42 The changes made in the amended whitepaper shall not extend the six-month time limit referred to in Paragraph CRA-15.1.39, unless approved by the CBB.

CRA-15.1.43 A supplementary whitepaper must conform to the following requirements:

(a) The order of the information appearing in the supplementary whitepaper must be consistent with that of the original whitepaper;

(b) Clear identification of the items/paragraphs it supplements or replaces;

(c) A statement that it is to be read in conjunction with the original whitepaper; and

(d) A responsibility statement from the Board of Directors of the digital token issuer.

CRA-15.1 Digital Token Offerings (continued)

CRA-15.1.44 The CBB shall make its decision with respect to the supplementary whitepaper, subject to any required changes, within 15 working days from receipt of all necessary documents and information complete in all aspects.

CRA-15.1.45 The supplementary whitepaper must be published and disseminated in manner as the original whitepaper. The document must contain the word "Supplementary Whitepaper" on the first page and describe the changes in relation to the original whitepaper.

CRA-15.1.46 An investor may withdraw subscription following publication of supplementary whitepaper. The withdrawals period of the subscription must be no less than six (6) business days from the date of publication of the supplementary whitepaper and the refund amount comprising the purchase price paid and any other charges imposed at the time of purchase of the digital token must be made within 5 business days from the date of refund request. No fee must be charged to the investor for the refund.

Dissemination of whitepaper

CRA-15.1.47 Upon approval by the CBB, the whitepaper must be made available to the investors at least 5 calendar days prior to the commencement of digital token offering.

CRA-15.1.48 The whitepaper must be effectively disseminated by posting it in an easily identifiable and accessible manner on the platform of the digital token advisor, as well as on the website of the digital token issuer in a downloadable format.

CRA-15.1.49 The whitepaper or the supplementary whitepaper, as disseminated and made available to the public by the digital token advisor, must be identical to the version approved by the CBB and must not undergo changes by the digital token issuer or the digital token advisor subsequent to the CBB's approval.

Marketing and Promotion

CRA-15.1.50 The marketing material for the digital token offering must be disseminated only after obtaining the CBB's approval.

CRA-15.1 Digital Token Offerings (continued)

CRA-15.1.51 A digital token issuer must not engage any third-party individual(s) or entity, other than the digital token advisor, to endorse or represent the digital token issuer with the intended purpose of marketing, promoting, gaining publicity or soliciting funds for its digital token offering.

CRA-15.1.52 The draft marketing material must be submitted to the CBB for approval and must:

(a) Indicate where the investor can obtain the whitepaper approved by the CBB by specifying the name of the website(s)/platform on which it is posted;

(b) State that investors should read the information contained in the whitepaper prior to making investment decisions;

(c) Be clearly identifiable as marketing material;

(d) Be fair, clear and not misleading;

(e) Disclose the risks related to the digital token offering; and

(f) Contain information that is consistent and does not contradict with the information provided in the whitepaper.

CRA-15.1.53 If, after the approval of the whitepaper by the CBB, the digital token issuer envisages to release marketing material whose content is substantially different from the marketing material submitted to the CBB prior to such approval, it must submit to the CBB the draft modified marketing material for approval.

CRA-15.1.54 Where a supplementary whitepaper is approved by the CBB, a modified version of the marketing material must be disseminated after seeking the prior approval of the CBB, in instances where the original marketing material is not in line with the changes made by the supplementary whitepaper.

CRA-15.1 Digital Token Offerings (continued)

Fees for Offering of Digital Tokens

CRA-15.1.55 **Offering of digital tokens is subject to fees levied by the CBB, pursuant to Article 180 of the CBB Law and Resolution No. (1) of 2007 with respect to determining fees categories due for licenses and services provided by the CBB. The following table outlines the non-refundable fees payable to the CBB, at the time of submission of an application for a digital token offering:**

Amount in BD

No.	Type of Approval	% of Offer Value	Min Amount	Max Amount
1.	Approval of the Whitepaper	0.025%	500	1250
3.	Supplementary Whitepaper	Fixed	100	100

CRA-15.1.56 An application for approval of a digital token offering and review of the documents related to the digital token offering will not be regarded as complete or submitted until the fee has been paid in full.

CRA-15.2 Digital Token Issuers Obligations

General Obligations

CRA-15.2.1 Digital token issuers must meet the following requirements:

(a) Appoint a digital token advisor to fulfil the obligations stipulated in this Module;

(b) Appoint a legal advisor for carrying out legal due diligence;

(c) Ensure that a robust corporate governance structure, which at a minimum includes necessary and appropriate policies, practices and internal controls, is in place to safeguard against unethical conduct, mismanagement and fraudulent activities;

(d) Put in place necessary systems and controls for mitigating the risks of money laundering and financing of terrorism. For this purpose, the digital token issuer must set up suitable organisational structures, internal procedures and a supervision system to address these risks and ensure compliance with its obligations relating to anti-money laundering and terror financing;

(e) Provide to the CBB any information or assistance as the CBB deems necessary relating to the digital tokens;

(f) Retain all relevant documents and agreements related to the digital token offering for a period of five (5) years; and

(g) Be liable towards its digital token holders for any damages incurred by them resulting from its wilful misconduct or negligence, including the failure to perform in whole or in part its obligations.

Governance Requirements

CRA-15.2.2 A digital token issuer must be headed by an effective Board. The size and composition of the Board should be commensurate with the size, nature and complexity of its business.

CRA-15.2.3 The Board is responsible for ensuring that the digital token issuer complies with the relevant provisions of the CBB Law, its regulations, resolutions and directives (including these Rules and other applicable Rules of the CBB Rulebook).

CRA-15.2.4 The Board has, both collectively and on an individual basis, an obligation to acquire and maintain sufficient knowledge and understanding of the digital token issuer's business to enable them to discharge their duties.

CRA-15.2 Digital Token Issuers Obligations (Continued)

CRA-15.2.5 The Board must:

(a) Act honestly and in good faith in the best interests of the digital token issuer and token holders;

(b) Exercise reasonable care, skill and diligence;

(c) Exercise the powers it has diligently and in line with applicable laws and not misuse such powers;

(d) Exercise its powers independently and without subordinating such powers to the will of others;

(e) Monitor, on an ongoing basis, the execution of the functions delegated to the digital token issuer's employees and be satisfied that they are performing their functions in accordance with their obligations;

(f) Identify and manage the risks relating to the digital token issuer and its activities;

(g) Monitor, on an ongoing basis, compliance with the relevant requirements of CBB Law, its regulations, resolutions and directives (including these Rules and other applicable Rules of the CBB Rulebook);

(h) Avoid conflicts of interest in so far as it is possible and, where it is not, ensure – inter alia by way of disclosure and internal conflicts of interest management procedures – that investors are treated fairly;

(i) Be responsible for the digital token issuer's compliance with the AML/CFT requirements; and

(j) Adopt a management structure commensurate with the digital token issuer's size, complexity, structure and risk profile.

CRA-15.2.6 A digital token issuer must ensure that its appointed senior management employees:

(a) Possess sufficient knowledge and expertise in the field of information technology, blockchain technology, digital tokens and their underlying technologies; and

(b) Maintain sufficient knowledge and understanding of the digital token issuer's business to enable them to discharge their function in a diligent manner.

CRA-15.2.7 Where a member of senior management leaves the organisation or is removed or replaced, such a change must be immediately disclosed to the digital token advisor and the digital token holders.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.2 Digital Token Issuers Obligations (Continued)

CRA-15.2.8 A digital token issuer must ensure that its Board and senior management are fit and proper, taking into account the following:

(a) They are suitably qualified to assume the position including having the relevant experience and track record in managing the business and affairs of the digital token issuer;

(b) They have not been disqualified to be a director by a court, regulator or any other competent authority;

(c) There is no pending criminal charge against the person in any court of law, whether within or outside Bahrain, for an offence involving fraud, integrity, dishonesty or mismanagement of an entity;

(d) They have not had any civil enforcement action initiated against them by any court of law or other competent authority, whether within or outside Bahrain;

(e) They have not:

(i) Been convicted, whether within or outside Bahrain, of an offence involving fraud, integrity, dishonesty other criminal conduct;

(ii) Been convicted of an offence under the securities laws or any other laws within or outside Bahrain relating to the capital market;

(iii) Contravened any provision of any law relating to a financial sector or companies in general, whether within or outside Bahrain involving dishonesty, incompetence, negligence, misconduct or malpractice;

(iv) Engaged in any business practices appearing to the CBB to be deceitful, oppressive or otherwise improper, whether unlawful or not, or which otherwise reflect discredit in the method of conducting business;

(v) Engaged in or has been associated with any other business practices or otherwise conducted himself in such a way as to cast doubt on his competence and soundness of judgement; or

(vi) Engaged in or has been associated with any conduct that cast doubt on his/her ability to act in the best interest of investors, having regard to the reputation, character, financial integrity and reliability.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.2 Digital Token Issuers Obligations (Continued)

CRA-15.2.9 **The digital token issuer, must submit a fit and proper declaration of its Board and senior management to:**

(a) The CBB at the time of submitting the application for offering of digital tokens; and

(b) The digital token advisor for any subsequent appointment to its board or senior management.

Digital Token Advisor Requirements

CRA-15.2.10 Prior to appointing a digital token advisor, the digital token issuer should review the ability of the digital token advisor to provide the service. While determining the suitability of a digital token advisor, the digital token issuer should consider the following:

(a) Historical record and prior performance;

(b) Availability of adequate systems, controls and resources to discharge its obligations in accordance with the CBB's requirement; and

(c) Suitably experienced and qualified employees having adequate knowledge and professional expertise to discharge its obligations.

CRA-15.2.11 **A digital token issuer must enter into a formal agreement with the digital token advisor by way of a signed letter of engagement defining clearly the extent of responsibilities and the terms of the agreement. The scope of the agreement must cover the obligations of the digital token advisor under the CBB rules in this regard.**

Repurchase of Digital Tokens

CRA-15.2.12 **If a digital token issuer has disclosed a digital token repurchase mechanism in the whitepaper, it may, after its digital tokens have been traded for a full year, carry out a repurchase (buyback) of its digital tokens, provided that it completes the execution of the buyback within 2 months from the day of making the public disclosure about the repurchase (buyback).**

CRA-15.2 Digital Token Issuers Obligations (Continued)

CRA-15.2.13 A digital token issuer must immediately cancel the digital tokens that it acquires under the digital token repurchase plan.

Periodic Reporting Requirements

CRA-15.2.14 Within 45 days after the end of each of the first 3 quarters, a digital token issuer must prepare a report in accordance with CRA-15.2.17 and publish it on the digital token advisor's platform.

CRA-15.2.15 A digital token issuer must prepare and publish a report, in accordance with CRA-15.2.16, on annual basis. The report must be published on the digital token advisor's platform within 60 days from the end of the financial year.

CRA-15.2.16 The digital token issuer's reports must contain information on the performance of the underlying business or project, including–

(a) Total amount of digital tokens issued and in circulation;
(b) Status of the utilisation of the digital token's proceeds by the digital token issuer;
(c) Status of the underlying business or project and any deviation from the whitepaper;
(d) Types of problems encountered, and the procedures applied or that will be applied to manage and resolve such problems;
(e) Risks facing the underlying business or project and measures taken for mitigation; and
(f) Unaudited quarterly financial statements reviewed by the external auditor for quarterly reporting and audited annual financial statements for annual reporting.

CRA-15.2 Digital Token Issuers Obligations (Continued)

CRA-15.2.17 **The financial statements must comply with International Financial Reporting Standards (IFRS). For Islamic institutions, audited financial statements must comply with AAOIFI standards or where AAOIFI standards do not cover a subject, IFRS must be followed.**

CRA-15.2.18 **A copy of the quarterly report and annual report referred to in Paragraphs CRA-15.2.15 and CRA-15.2.16 must be filed with the CBB no later than the date of its publication.**

Disclosure of Material Information

CRA-15.2.19 **A digital token issuer must immediately disclose information regarding any material matter/event on the appointed digital token advisor's platform. Information would be regarded as material if its omission or misstatement could change or influence the assessment or decision of an investor relying on that information for the purpose of making economic decisions.**

CRA-15.2.20 For the purposes of CRA-15.2.19, the following are examples of events that are to be considered material:

(a) Loss of creditworthiness;
(b) Searches and seizures by law enforcement authorities, any litigious or non-litigious matter, administrative disposition, administrative litigation, precautionary injunctive procedure, or compulsory execution, with a material effect on the finances or business or project of the digital token issuer;
(c) Major decrease in operations or a full or partial work stoppage;
(d) A pledge/lien on all or a major portion of its assets;
(e) Amendment, termination, or rescission of memorandum and articles of association;
(f) A plan for strategic alliance or other business cooperation plan or important contract, or a change in important content of a business plan, or purchase of an enterprise, or acquisition of or assignment to another of patent rights, trademark rights, copyrights, or other intellectual property related transactions, with a material effect on the finances or business or project of the digital token issuer;
(g) Occurrence of a disaster, protest, strike, environmental pollution event, information security incident, with a material effect on the finances or business of the digital token issuer;
(h) The resignation, dismissal or appointment of any key Board/management personnel;
(i) Material changes to the equity holding held by the board of directors or senior management;

CRA-15.2 Digital Token Issuers Obligations (Continued)

(j) Change in the registered office address, legal name, financial year-end, or external auditor;
(k) Resolution by the board of directors to repurchase (buyback) digital tokens, expiration of a repurchase (buyback) period, or completion of execution of a repurchase (buyback);
(l) Resolution by the board of directors to apply for termination of trading of the issuer's digital tokens on the trading platform; and
(m) Announcement of suspension or termination of trading of the digital tokens on the trading platform.

CRA-15.2.21 **To ensure equal access to information, a digital token issuer must not externally disclose any material information on its own before publishing it on the appointed digital token advisor's platform.**

CRA-15.2.22 **If there is any material change in the development of subsequent events with respect to material information that a digital token issuer has already published, the digital token issuer must update or supplement in a timely manner the content of the relevant information in accordance with the procedure under which the information was originally disclosed.**

Power of the CBB to issue Direction

CRA-15.2.23 **The CBB may at any time issue a direction to the digital token issuer which must be complied with, if the CBB:**
(a) is of the view that it is necessary for the:
(i) purposes of ensuring fair and orderly market; or
(ii) purposes of the protection of the holders of digital tokens, or in the public interest; or
(b) is of the opinion that the underlying project or business is no longer viable or sustainable.

CRA-15.2.24 A direction issued under Paragraph CRA-5.2.23 may include a direction:
(a) Not to deal or transfer monies or properties to any other person;
(b) Not to solicit business from any person;
(c) To cease or refrain from committing an act or pursuing a course of conduct or activity;
(d) To do any act, in relation to its business, affairs, property, project or digital token as the CBB deems necessary;
(e) To give effect to any requirement of the applicable laws, rules and regulations; or
(f) Relating to other matter as the CBB considers necessary

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.3 Role and Responsibilities of Digital Token Advisor

CRA-15.3.1 This section sets the role and responsibility of a category-3 or category-4 crypto-asset licensee acting as a digital token advisor to a digital token issuer.

CRA-15.3.2 Digital token issuers must appoint either a category-3 or a category-4 crypto-asset licensee as digital token advisor. The digital token advisor must ensure that the digital token issuer satisfies all requirements as prescribed under the CBB Law, its regulations, resolutions and directives (including this Chapter and other applicable rules of the CBB Rulebook).

Independence and Avoidance of Conflict of Interest

CRA-15.3.3 A digital token advisor must be independent from the digital token issuer. A confirmation in writing of its independence must be submitted to the CBB. A digital token advisor will not be considered independent by the CBB if:

(a) It has ownership interest in the digital token issuer or any other company within the digital token issuer's group;

(b) It has a business relationship with, or financial interest in, the digital token issuer or any other entity in the digital token issuer's group that would give the digital token advisor, or the digital token advisor's group, a material interest in the outcome of the transaction; or

(c) A director or employee of the appointed digital token advisor or another entity in the appointed digital token advisor's group, has a material interest in the digital token issuer or any other entity in the digital token issuer's group.

CRA-15.3.4 A digital token advisor's directors and shareholders must disclose to the investors on its platform if they hold any shares in any of the issuers hosted on its platform.

CRA-15.3.5 A digital token advisor is prohibited from providing direct or indirect financial assistance to investors, to invest in digital tokens.

CRA-15.3 Role and Responsibilities of Digital Token Advisor (Continued)

Obligations of Digital Token Advisor

CRA-15.3.6 A digital token advisor must:

(a) Ensure that the digital token issuer satisfies all the requirements as applicable for offering of digital tokens;

(b) Advise and guide the digital token issuer as to its responsibilities and obligations to ensure compliance with the CBB Law, its regulations, resolutions and directives (including these Rules and other applicable Rules of the CBB Rulebook) and all other applicable laws;

(c) Exercise its own judgment and carry out assessment on the digital token issuer's compliance with the requirements of Chapter CRA-15 including as to whether the digital token issuer will be able to satisfy the requirement to provide an innovative solution or a meaningful security value proposition;

(d) Appoint an eligible CBB licensed retail bank for deposit of all funds raised through the digital token issue;

(e) Submit to the CBB all required information and documentation including the documents required for assessment of the digital token offer, in a timely manner;

(f) Carry out due diligence on a digital token issuer including:

(i) Understanding and verifying the business and project of the digital token issuer to ensure that the digital token issuer does not engage in any business practices appearing to be deceitful, oppressive or improper, whether unlawful or not;

(ii) Conduct background checks on the issuer's board and senior management to ensure "fit and proper" requirements are met by the digital token issuer;

(iii) Understand the features of the digital token to be issued by the digital token issuer and the rights attached to it;

(iv) Assess the digital token issuer's whitepaper as well as other documents as stated in Chapter CRA-15. In assessing the digital token issuer's whitepaper as well as other documents, the digital token advisor must ensure that the contents of the aforementioned documents include the information required under Chapter CRA-15 and that its contents are fair, accurate, complete, clear, not misleading and there are no material omissions.

CRA-15.3 Role and Responsibilities of Digital Token Advisor (Continued)

(g) Disclose to the CBB, without delay, any information or explanations that the CBB may reasonably require for the purpose of verifying any information which should be taken into account in considering an application for registration of a whitepaper; and

(h) Act as liaison between the digital token issuer and the CBB on all matters arising in connection with the registration of the whitepaper or the trading of the issuer's digital token on the crypto-asset exchange platform.

CRA-15.3.7 In addition to the obligations set out in Paragraph CRA-15.3.6, a digital token advisor must:

(a) Make the digital token issuer's whitepaper accessible to investors through its electronic platform;

(b) Must make available through its electronic platform all relevant information relating to a digital token issuer including any material changes that are affecting the digital token issuer or the digital token issuer's project;

(c) Take reasonable steps in monitoring the drawdowns by digital token issuer and that it has been utilised for the purposes stated in the whitepaper;

(d) Ensure that its electronic platform is operating in an orderly, fair and transparent manner;

(e) Have in place rules and procedures for the offering of digital tokens on its electronic platform;

(f) Ensure that all fees and charges payable are fair, reasonable and transparent;

(g) Take all reasonable measures to avoid situations that are likely to involve a conflict of interest with the digital token issuer and establish and maintain policies and procedures to effectively and efficiently manage actual and potential conflicts of interest, including the management of non-public material information and conflicts with the digital token issuer;

(h) Ensure that all disclosures are fair, accurate, clear and not misleading; and

(i) Provide any information or document to the CBB as it may require.

CRA-15.3 Role and Responsibilities of Digital Token Advisor (Continued)

CRA-15.3.8 A digital token advisor must immediately notify the CBB if any of the following has occurred:

(a) Any breach of the provisions of the CBB Law, its regulations, resolutions and directives (including these Rules and other applicable Rules of the CBB Rulebook); and

(b) Any material adverse change to the digital token issuer including, but not limited to, any of the following matters:

(i) The discovery of a false or misleading statement in any disclosures in relation to the digital token offer;

(ii) The discovery of any material omission of information that may affect digital token holders; and

(iii) There is a material change or development in the circumstances relating to the digital token offering or the digital token issuer.

Supplementary Whitepaper

CRA-15.3.9 Where a supplementary whitepaper has been submitted by a digital token issuer to the CBB, the digital token advisor must notify the subscribers for the digital token regarding the filing of the supplementary whitepaper with the CBB and that the supplementary whitepaper will be made available on the electronic platform upon approval of the CBB.

CRA-15.3.10 Upon approval of the CBB, the supplementary whitepaper must be made available on the electronic platform of the digital token advisor.

CRA-15.3.11 Where a subscriber, pursuant to publication of supplementary whitepaper, wishes to withdraw his/her subscription for the digital token, the withdrawal period of the subscription and the refund period must be in accordance with Chapter CRA-15.

Register of Initial Digital Token Holders

CRA-15.3.12 A digital token advisor must maintain a register of initial digital token holders who subscribed for the digital tokens during the offer period and enter into the register the total amount of digital tokens subscribed by each digital token holder.

CRA-15.3 Role and Responsibilities of Digital Token Advisor (Continued)

Record of Digital Token Holders Monies and Digital Tokens

CRA-15.3.13 **A digital token advisor must establish systems and controls for maintaining an accurate and up to date record of digital token holders and any monies or digital tokens held in relation to them.**

CRA-15.3.14 A digital token advisor must ensure that records pertaining to register of initial digital token holders is maintained in an easily retrieval format for examination by the CBB.

Custody of Digital Tokens

CRA-15.3.15 **The digital token advisor must maintain custody of the digital tokens issued by the digital token issuer on its platform. At a minimum, the custodial arrangement must meet the requirements stipulated in Chapter CRA-8 of this Module.**

CRA-15.3.16 **A digital token advisor must ensure digital tokens held under a custody arrangement are properly safeguarded from conversion or inappropriate use by any person, including, but not limited, to implementing multi-signature arrangements.**

Investor Money

CRA-15.3.17 **Subscription monies received in respect of the digital token offer must be held in a separate bank account under an escrow arrangement with a licensed retail bank in Kingdom of Bahrain.**

CRA-15.3.18 **The release of funds to the digital token issuer must be done in accordance with the provisions stipulated in Chapter CRA-15.**

CRA-15.3.19 A digital token advisor may impose any other additional conditions before releasing the funds, provided that the additional conditions serve the interest of the digital token holders.

CRA-15.3 Role and Responsibilities of Digital Token Advisor (Continued)

Fund Monitoring and Safeguarding Arrangement

CRA-15.3.20 Digital token advisors must have in place a fund monitoring and safeguarding arrangement for the funds raised through the digital token offering which must include:

(a) The subscription money (client money) be received into a client money account with a retail bank in Bahrain and make clear in the title of the account that the funds in the account belong to one or more clients of the licensee and not to the licensee:

(i) Held in a segregated client money account;

(ii) Held in a fiduciary capacity and must not be commingled with its own funds;

(iii) Used only for the purposes for which the licensee received it from its clients;

(iv) Not used for licensee's own use at any point in time or given as collateral for any purpose to a third party or be subject to any restrictions;

(v) Reported separately as on balance sheet item in the licensee's financial statements specifying also the nature and purpose for which such funds are held by the bank on behalf of its customers; and

(b) Procedures for collection and management of the funds including procedures for the utilisation, refund and release of funds.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.4 Trading and Settlement of Digital Tokens

CRA-15.4.1 Trading of digital tokens can be conducted either by:

(a) Operating an automated order matching system (exchange type order matching engine) by a category-4 crypto-asset exchange licensee, wherein buyer and seller orders are automatically matched by the matching engine and the crypto-asset exchange does not buy or sell digital tokens over-the-counter (acting as a dealer); or

(b) Over-the-counter trading, wherein a category-3 or a category-4 crypto-asset licensee acts as a dealer and provides price quotes, on its trading platform, with its clients for the digital tokens issued and listed on its platform.

CRA-15.4.2 A digital token must not be simultaneously listed on the same platform for both types of trading i.e. order matching type market (buyer and seller orders are matched automatically by a matching engine) and over-the-counter trading market.

Over-the-counter Trading

CRA-15.4.3 Category-3 and category-4 crypto-asset licensees must establish written rules for over-the-counter trading of digital tokens and publish them on its trading platform.

CRA-15.4.4 The over-the-counter trading rules referred to in Paragraph CRA-15.4.3 must include the trading platform's business days and trading hours, price quote method, trade execution principles, price stabilization mechanism, trading procedures, method for the advance collection of purchase prices and digital tokens to be sold, upper and lower price limit for trading, conditions under which trading halt (circuit breaker) shall be imposed, and the handling of settlement and default.

CRA-15.4.5 Category 3 and category-4 crypto-asset licensees engaging in over-the-counter trading of digital tokens with clients on its trading platform must collect in advance from a client the full amount of the purchase price or the digital tokens to be sold.

CRA-15.4.6 Category 3 and category-4 crypto-asset licensees undertaking over-the-counter trading of digital tokens must open a dedicated account at a licensed bank in Kingdom of Bahrain for the collection and payment of funds.

CRA-15.4 Trading and Settlement of Digital Tokens (continued)

CRA-15.4.7 Category 3 and category-4 crypto-asset licensees engaging in over-the-counter trading of digital tokens must provide two-way, buy and sell, quotes.

CRA-15.4.8 Category 3, and category-4 crypto-asset licensees, undertaking over-the-counter trading of digital tokens, must provide reasonable price quotes based on its professional judgment and must efficiently adjust demand and supply in the market depending on the market situation and must not give a quote that deviates from a reasonable price, thereby impairing the formation of fair prices.

CRA-15.4.9 Where a category 3, category-4 crypto-asset licensee engages in over-the-counter trading of digital tokens with its clients on its trading platform, the aggregate trading volume of the purchases and sales of any single digital token on any single business day must not exceed 50 percent of the issued quantity of that digital token.

CRA-15.4.10 Category 3 and category-4 crypto-asset licensees undertaking over-the-counter trading of a digital token with its clients on its trading platform, must disclose on the trading platform relevant information to take informed trading decision including price, quantities and other trade information.

CRA-15.4.11 The trade information referred to in Paragraph CRA-15.4.10 must, at a minimum, include the price and quantity of the most recent trade, the cumulative trading volume, and highest, lowest, and weighted average trading price, of the digital token during the trading hours.

CRA-15.4.12 After the close of daily trading hours, category 3 and category-4 crypto-asset licensees must prepare and disclose the trading volume and weighted average trading price of each digital token on that day.

CRA-15.4.13 The CBB may, at any time, by notice in writing to a category 3, category-4, vary any condition or restriction or impose such further condition or restriction as it may deem fit including but not limited to suspension of trading or termination of trading of a digital token.

CRA-15.4.14 Category-3 and category-4 crypto-asset licensee undertaking over-the-counter trading must adhere to conduct of business obligations as stipulated in Section CRA-12 of this Module.