CRYPTO-ASSET MODULE

MODULE:	CRA (Crypto-asset)

Table of Contents

Table of Contents (continued)

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 ~~accepted~~ 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) ~~Users' guide;~~
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) 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	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 requirements on 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-5.8.3 & CRA-5.8.5	01/2020	Amended Paragraphs on approval of the banks policies and procedures.
CRA-5.8.19A	01/2020	Added 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 requirements for periodic assessments of cyber security threats.
CRA-5.8.28-CRA-5.8.29	01/2020	Added requirement for cyber security insurance.
CRA-7.1.1A	01/2020	Added 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 reference to Module AML and removed transaction record details.

Effective Date

CRA-A.2.1 **The contents of this Module are effective from the date of release of the Module or the changes to the Module unless specified otherwise.**

MODULE	CRA:	Crypto-asset
CHAPTER	CRA-B	Scope of Application

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 regulations for 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.1.5 A person who contravenes the provisions of this Module or other applicable Modules shall be liable for financial penalties and enforcement actions stipulated under the various provisions of the CBB Law including, but not limited to, criminal sanctions, fines, imprisonment, suspension of license, public censure, freezing of accounts, cease and desist order and specific directives.

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 A person would be considered in breach of CRA-1.1.2 if the person attempts to operate as, or incorporate a company in Bahrain with a name containing the words (or the equivalents in any language) "crypto", "digital", "currency", or "asset" in combination with "exchange", "manager", "adviser", "investment", or "portfolio", without holding the appropriate CBB license or the prior approval of the CBB.

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 ~~accepted~~ crypto-assets and the transmission of that order to a third party for execution.

(b) Execution of orders on behalf of clients: Acting to conclude agreements to buy and/or sell for one or more ~~accepted~~ crypto-assets on behalf of the clients.

(c) Dealing on own account: Trading against proprietary capital resulting in conclusion of transactions in one or more ~~accepted~~ crypto-assets.

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

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

(f) Investment Advice: Giving, offering or agreeing to give, 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 ~~accepted~~ 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 ~~accepted~~ crypto-asset, or hold a particular ~~accepted~~ crypto-asset. A recommendation is not a "personal recommendation" if it is issued exclusively through distribution channel or to the public.

(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) ~~accepted~~ crypto-assets for fiat currency or vice versa; and/or
(ii) ~~accepted~~ crypto-assets for another ~~accepted~~ 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 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 or administration of crypto assets;
(b) the development, dissemination or use of software for the purpose of creating or mining a crypto asset; ~~or~~
(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:

(i) Reception and transmission of orders;
(ii) Provide investment advice in relation to ~~accepted~~ 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:

(i) Trading in ~~accepted~~ crypto-assets as agent;
(ii) Portfolio Management;
(iii) Crypto-asset custody;
(iv) 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:

(i) Trading in ~~accepted~~ crypto-assets as agent;
(ii) Trading in ~~accepted~~ crypto-assets as principal;

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

(iii) Portfolio Management;
(iv) Crypto-asset custody;
(v) Investment advice.

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:
(i) Operate a licensed crypto-asset exchange;
(ii) Crypto-asset custody service;
(iii) 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 approved for the trading of the digital token under the over-the-counter trading framework.

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

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.**

CRA-1.1.19 **An application for a license must be in the form prescribed by the CBB and must contain, *inter alia*:**
(a) A business plan specifying the type of business to be conducted;
(b) Application forms for all shareholders and subsidiaries; and
(c) Application forms for all controlled functions.

CRA-1.1.20 The CBB will review the application and duly advise the applicant in writing when it has:
(a) Granted the application without conditions;
(b) Granted the application subject to conditions specified by the CBB; or
(c) Refused the application, stating the grounds on which the application has been refused and the process for appealing against that decision.

CRA-1.1.21 Detailed Rules and guidance regarding information requirements and processes for licenses can be found in Section CRA-1.2. As specified in Paragraph CRA-1.2.13, the CBB will provide a formal decision on a license application within 60 calendar days of all required documentation having been submitted in a form acceptable to the CBB.

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 License for crypto-asset service (continued)

Combining Regulated Crypto-asset Services

CRA-1.1.23 Licensees may combine two or more regulated crypto-asset services, provided these fall within the permitted list of services and such combinations does not create possible conflict of interest.

CRA-1.1.24 Those seeking a license should satisfy the CBB as to their suitability to carry out the regulated crypto-asset services for which they are seeking license.

CRA-1.1.25 In assessing applications for a license, the CBB will assess whether an applicant satisfies the licensing conditions (as specified in Chapter CRA-2) with respect to all the regulated services that the applicant proposes to undertake.

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-1.1.27 Category 1, Category 2 and Category 3 crypto-asset licensees are required to design and structure its operations, user interface, website, marketing materials and any public or client-facing information such that it does not create the impression that it is running a licensed crypto asset exchange. In practice, category 1, category 2 and category 3 crypto-asset licensees must not (i) display any publicly-accessible information that may appear like a trading order book, (ii) not provide for any price discovery, and (iii) not giving 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 Articles 44 to 47 of the CBB Law govern the licensing process which also stipulates that the CBB will take a decision within 60 calendar days of an application being deemed complete (i.e. containing all required information and documents). See below, for further details on the licensing process and time-lines

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) For overseas companies, a copy of the company's current commercial registration, license from competent authority and/or equivalent documentation;
(e) Where the applicant is an existing Bahraini company, 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) In the case of branch applicants, a letter of non-objection to the proposed license application from the applicant's home supervisor, together with confirmation that the applicant is in good regulatory standing and the company concerned is in compliance with applicable supervisory requirements, including those relating to capital;

(i) In the case of branch applicants, copies of the audited financial statements of the applicant (head office) for the three years immediately prior to the date of application;

(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 either (i) or (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;

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

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

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 as mentioned in 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;

(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;

(d) The proposed Board and senior management of the applicant and the proposed organisational structure of the applicant;

(e) An ~~independent~~ 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; and

(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) A copy of its business continuity plan; and

(h) 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-1.2.7 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 Application for License (continued)

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 By law, the 60 days' time limit referred to in Paragraph CRA-1.2.2 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-1.2.13 Therefore, applicants may first submit an unsigned Form 1 in draft, together with as many as possible of the items specified in Rule CRA-1.2.4. This draft application should contain at least items in Rule CRA-1.2.4(a); Rule CRA-1.2.4(b), with respect to proposed Directors (but not necessarily senior management); Rule CRA-1.2.4(c); Rule-CRA-1.2.4(d); and Rule CRA-1.2.4(g) to Rule CRA-1.2.4(m) inclusive.

CRA-1.2.14 On the basis of the information specified in Paragraph CRA-1.2.13, the CBB may provide an initial 'in principle' confirmation that the applicant appears likely to meet the CBB's licensing requirements, subject to the remaining information and documents being assessed as satisfactory. The 'in principle' confirmation will also list all outstanding documents required before an application can be considered complete and subject to formal consideration.

CRA-1.2 Application for License (continued)

CRA-1.2.15 An 'in principle' confirmation does not constitute a license approval, nor does it commit the CBB to issuing a license. However, it provides sufficient assurance for an applicant to complete certain practical steps, such as securing suitable executive staff that satisfy CBB's 'fit and proper' requirements. Once this has been done, the applicant may finalise its application, by submitting the remaining documents required under Rule CRA-1.2.1 and, once assessed as complete by the CBB, a signed and dated final version of Form 1. However, a Bahraini company proposing to undertake financial services activities would not be eligible to obtain a Commercial Registration from the Ministry of Commerce, Industry and Tourism unless it receives the final approval from the CBB.

CRA-1.2.16 Regardless of whether an applicant submits a draft application or not, 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 (either in draft or in final).

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-1.2.18 **An applicant must not hold himself out as having been licensed by the CBB, prior to receiving formal written notification of the fact in accordance with Rule CRA-1.2.19 below. Failure to do so may constitute grounds for refusing an application and result in a contravention of Articles 40 and 41 of the CBB Law (which carries a maximum penalty of BD 1 million).**

CRA-1.2 Application for License (continued)

Granting or Refusal of License

CRA-1.2.19 To be granted a license, an applicant ~~must~~ should demonstrate compliance with the applicable requirements of the CBB Law, this Module as well as other applicable modules of Volume 6. 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 refuse to grant a license if in its opinion:

(a) The requirements of the CBB Law or this Module 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~~ should 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 The CBB may conduct an examination or seek further information to ascertain the readiness of the licensee to commence operation, even if a readiness assessment report has been submitted to the CBB.

Commencement of Operations

CRA-1.2.26 **Prior to commencement of operation ~~Within 6 months of the license being issued,~~ 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) The address in Bahrain where full business records will be kept;
(c) The licensee's contact details including telephone and fax number, e-mail address and website;
~~(d) A copy of its business continuity plan;~~
~~(e) A description of the IT system that will be used, including details of how IT systems and other records will be backed up;~~
(f) A copy of the auditor's acceptance to act as auditor for the applicant;
(g) A copy of an auditor's opinion certifying that the licensee's capital – as specified in the business plan submitted under Rule CRA-1.2.4 has been paid in;
(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;

CRA-1.2 Application for License (continued)

(j) A copy of the commercial registration certificate in Arabic and in English from the Ministry of Commerce, Industry and Tourism;

(k) A copy of the licensee's business card and any written communication (including stationery, website, e-mail, business documentation, etc.) including a statement that the company is licensed by the CBB; ~~and~~

(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 **Upon receipt of a license from the CBB, the licensee must commence their commercial operations within 6 months of being granted a license by the CBB, failing which the CBB may cancel the license, as per the powers and procedures set out in Article 48 of the CBB Law.**

CRA-1.2.28 The procedures for amending or cancelling licenses are contained in Sections CRA-1.3.

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 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-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 Failure to comply with Rule CRA-1.3.1 may constitute a breach of Article 50(a) of the CBB Law. The CBB will only approve such a request where it has no outstanding regulatory concerns and any relevant client interests would not be prejudiced. A voluntary surrender of a license will not be accepted where it is aimed at pre-empting supervisory actions by the CBB. A voluntary surrender will only be allowed to take effect once the licensee, in the opinion of the CBB, has discharged all its regulatory responsibilities to clients.

Cancellation of a License by the CBB

CRA-1.3.4 As provided for under Article 48 (c) of the CBB Law, the CBB may itself move to cancel a license, for instance if a licensee fails to satisfy any of its existing license conditions or protecting the legitimate interests of clients or creditors of the licensee require a cancellation. 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 Cancellation of a license requires the CBB to issue a formal notice of cancellation to the licensee concerned. The notice of cancellation describes the CBB's rationale for the proposed cancellation, as specified in Article 48(d) of the CBB Law.

CRA-1.3.6 Where the cancellation of a license has been confirmed by the CBB, 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.

CRA-1.3 Cancellation or Amendment of License (continued)

Amendment of license

CRA-1.3.7 Licensees wishing to vary the scope of their license must obtain the CBB's written approval, before effecting any such change. Approval must be sought whenever a licensee wishes to add or cease undertaking a regulated crypto-asset service, change license category or to vary a condition imposed on their license.

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 There are no application fees for those seeking approved person status.

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 Licensees failing to comply with this Section may be subject to financial penalties as prescribed by the CBB or may have their licenses withdrawn by the CBB.

CRA-1.7 Approved Persons

General Requirements

CRA-1.7.1 **Licensees must obtain the CBB's prior written approval for any person wishing to undertake a controlled function in a licensee. The approval from the CBB must be obtained prior to their appointment, subject to the variations contained in Paragraphs CRA-1.7.3 and Paragraph CRA-1.7.4.**

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 **In the case of Bahraini regulated crypto-asset service licensee, prior approval is required for all of the above controlled functions. Combination of the above controlled functions is subject to the requirements contained in Paragraph MIR-3.1.3 of Module MIR.**

CRA-1.7.4 **In the case of overseas crypto-asset service licensees, prior approval is required for controlled function (b) defined as the 'Branch Manager' of the Bahrain branch (however titled by the licensee), (c), (d), (e) and (f). Combination of the above controlled functions is subject to the requirements contained in Paragraph MIR-3.1.3 of Module MIR.**

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 three of the controlled functions (i) Directors, (ii) Chief Executive or General Manager and (iii) Money Laundering Reporting Officer.

CRA-1.7 Approved Persons (continued)

CRA-1.7.6 Pursuant to CRA-1.7.5, a licensee seeking exemption from appointment of persons to specific controlled functions must 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 be made will be managed; 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

(b) 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.

Basis for Approval

CRA-1.7.7 **For the purposes of Paragraph CRA-1.7.1, licensees must adhere to the requirements for authorisation of approved persons as set out under Sections MIR-3.1, MIR-3.2, MIR-3.3, MIR-3.4, MIR-3.5 and MIR-3.6 under Module MIR except for Rule MIR-3.1.2 and MIR-3.1.2A.**

CRA-1.7.8 Approval under Paragraph CRA-1.7.1 is only granted by the CBB, if it is satisfied that the person is fit and proper to hold the particular position in the licensee concerned. 'Fit and proper' is determined by the CBB on a case-by-case basis. The definition of 'fit and proper' and associated guidance is provided in Sections MIR-3.3 of Module MIR.

CRA-1.7 Approved Persons (continued)

Cancellation of Approved Person Status

CRA-1.7.9 **In accordance with Paragraphs MIR-3.4.11 of Module MIR and CRA-10.2.12, licensees must promptly notify the CBB in writing when a person undertaking a controlled function will no longer be carrying out that function. 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-1.7.11 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: see Chapter MIR-3.6 of Module MIR regarding the cancellation of 'fit and proper' approval.

CRA-1.7.12 A Director is any person who occupies the position of a Director, as defined in Article 173 of the Commercial Companies Law (Legislative Decree No. 21 of 2001).

CRA-1.7.13 The fact that a person may have 'Director' in his job title does not of itself make him a Director within the meaning of the definition noted in Paragraph CRA-1.7.12. For example, a 'Director of Marketing', is not necessarily a member of the Board of Directors and therefore may not fall under the definition of Paragraph CRA- 1.7.12.

CRA-1.7 Approved Persons (continued)

CRA-1.7.14 **Licensees must appoint a person to undertake the function of Chief Executive or General Manager. The Chief Executive or General Manager means a person who is responsible for the conduct of the licensee (regardless of actual title). The Chief Executive or General Manager must be resident in Bahrain. This person is responsible for the conduct of the whole of the firm, or, in the case of an overseas crypto-asset ~~exchanger~~ licensee, for all of the activities of the branch.**

CRA-1.7.15 **The Chief Executive or General Manager of the licensee:**

(a) Must be fully responsible for the executive management and performance of the licensee, within the framework of delegated authorities set by the Board;

(b) Must devote full-time working hours to the licensee; and

(c) Must not be employed at any other firm.

CRA-1.7.16 Residency requirements apply to Chief Executives, General Managers or Managing Directors as well as for other controlled functions as specified in Section CRA-2.2.

CRA-1.7.17 Head of function means a person who exercises major managerial responsibilities, is responsible for a significant business or operating unit, or has senior managerial responsibility for maintaining accounts or other records of the licensee.

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.

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) A branch resident in Bahrain of a company incorporated under the laws of its territory of incorporation.

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

(i) A Bahraini joint stock company (B.S.C.); or
(ii) A branch resident in Bahrain of a company incorporated under the laws of its territory of incorporation.

CRA-2.1.2 Where the application is for establishing a branch of an overseas crypto-asset service licensee, an application for licensing will be considered after extensive enquiries into the firm's shareholders, management structure, financial position, its activities and how these activities are regulated.

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. Overseas crypto-asset service licensees must maintain a local management presence and premises in the Kingdom appropriate to the nature and scale of their activities.

CRA-2.2.2 The CBB requires that all approved persons occupying controlled functions outlined in Paragraph CRA-1.7.2, except for Sub-paragraph CRA-1.7.2(a) must be resident in Bahrain.

CRA-2.2.3 Overseas crypto-asset service licensees must seek the CBB's prior approval if some of its controlled functions are resident outside of Bahrain.

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 is contained in Section CRA 1.7, whilst Sections MIR -3.1 to MIR- 3.6 of Module MIR sets out CBB's approved person requirements. Applications for approved person status must be submitted using the prescribed approved persons form.

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 exceed at all times the minimum requirements contained in Chapter CRA-3.

CRA-2.5.2 Overseas applicants are required to provide written confirmation from their head office in the form of an undertaking that the head office will provide financial support to the branch sufficient to enable it to meet its obligations as and when they fall due. Overseas applicants must also demonstrate that the company as a whole is adequately resourced for the amount of risks undertaken.

CRA-2.6 Condition 6: Systems and Controls

CRA-2.6.1 Licensees must maintain systems and controls that are, in the opinion of the CBB, 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, in the opinion of the CBB, 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 As part of the licensing approval process, applicants must demonstrate in their business plan (together with any supporting documentation) what risks their business would be subject to and how they would manage those risks.

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 Module MIR.

CRA-2.6.6 Licensees providing custody services specified in Paragraph CRA-1.1.6(e), must segregate the personnel, systems and controls to avoid conflicts of interest with other activities undertaken as specified under Paragraph CRA-1.1.6.

CRA-2.6.7 Licensees must additionally comply with the systems and controls requirements set out in Module MIR in Section 4, of the CBB Rulebook Volume 6.

CRA-2.7 Condition 7: External Auditor

CRA-2.7.1 As per 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 as set out in MIR-4.8 of Module MIR of the CBB Rulebook Volume 6.

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 comply with the minimum record-keeping requirements contained in Section MIR-4.6 of Module MIR. Books of accounts must comply with International Financial Reporting Standards (IFRS) and, in the case of Sharia compliant crypto asset service licensees, the Accounting and Auditing Standards of the Accounting and Auditing Organisation for Islamic Financial Institutions (AAOIFI) the relevant requirements set out in Module MIR in Section 4.6, of the CBB Rulebook Volume 6.**

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 initial capital, which is 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;
(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 ~~accepted~~ crypto assets as principal and thereby taking proprietary positions in ~~accepted~~ 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 Overseas crypto-asset service licensees must calculate their Minimum Capital Requirements in accordance with the requirements that would be applicable if they were a joint stock company incorporated in Bahrain. Overseas crypto-asset service licensee must ensure compliance with the minimum capital requirements specified in Rule CRA-3.1.2.

CRA-3.2.3 As specified in 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;
(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 ~~accepted~~ 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 ~~publishing in the press,~~ the ~~draft agenda for any~~ shareholders' meetings referred to in Paragraph CRA-4.1.1 (r);

(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 (i.e. ordinary and extraordinary general assembly) taking 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(r), provide to the CBB a copy of the minutes of the meeting.

(t) 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.

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. Such measures must, among others, include keyman insurance or other similar cover.

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 and not licensed by the CBB about any associated risks.

CRA-4.1.4 Licensees must use appropriate technology and wherever appropriate third-party services to identify the following situations, and other additional mitigating or preventive actions as necessary to mitigate the money laundering and terror financing risks involved:

(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

CRA-4.1 General Obligations (continued)

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

a) For suitability assessment:

(i) Client's knowledge and experience:

- the types of investment services and transaction which the client is familiar;
- the nature, volume, frequency of the client's transactions with trading and investments; and
- the level of education, profession or (if relevant) former profession of the client.

(ii) Client's financial situation:

- the source and extent of the client's regular income;
- the client's assets, including liquid assets, investments and real property;
- the client's regular financial commitments;
- the ability to bear losses.

CRA-4.1 General Obligations (continued)

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

b) For appropriateness assessment:

(i) Client's knowledge and experience in order to enable the licensee to determine whether the crypto-asset products and services are appropriate:
- the types of investment services and transaction which the client is familiar;
- the nature, volume, frequency of the client's transactions with trading and investments; and
- the level of education, profession or (if relevant) former profession of the client.

Transaction with Unknown Counterparties

CRA-4.1.9 **A licensee must 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 In accordance with Article 61 of the CBB Law, licensees must appoint auditors and comply with the provisions of Section MIR-4.8 of Module MIR.

CRA-4.2.1A 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-4.2.2 Audited financial statements of a licensee must be prepared in accordance with the International Financial Accounting Standards (IFRS) or AAOIFI standards as appropriate.

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.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-4 Business Standards and Ongoing Obligations

CRA-4.3 Listing of ~~Accepted~~ Crypto-assets

CRA-4.3.1 ~~**The CBB has the authority to determine the suitability of a crypto-asset for the purposes of undertaking regulated crypto-asset services.**~~

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

~~CRA-4.3.2~~ ~~**Licensees must undertake regulated crypto-asset services in accepted crypto-assets only., after seeking prior written approval of the CBB. Licensees wishing to use a crypto-asset(s) in addition to the already accepted crypto-asset(s) originally approved as part of its application process, must provide a notification to the CBB of its intention to do so and provide with it all relevant information relating to the crypto-asset, the exchanges on which it is traded and the additional systems and controls the licensee has or will establish in order to manage the risks specific to the crypto-asset.**~~

CRA-4.3.2A **Licensees are only 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. Licensees should approach the CBB and seek a written approval prior to offering derivative products.

~~CRA-4.3.3~~ ~~The CBB will consider a number of factors while approving accepted crypto-assets, including those mentioned below:~~

~~(a) The technological experience, track record and reputation of the issuer and its development team;~~

~~(b) The issuer's AML/CFT and cybersecurity systems and controls;~~

~~(c) The availability of a reliable multi-signature hardware wallet solution for the asset;~~

~~(d) The protocol and the underlying infrastructure, including *inter alia* whether it is: (i) a separate Blockchain with a new architecture system and network or it leverages an existing Blockchain for synergies and network effects, (ii) scalable, (iii) new and/or innovative or (iv) the crypto-asset has an innovative use case or application;~~

~~(e) The relevant consensus protocol;~~

~~(f) Developments in markets in which the issuer operates;~~

CRA-4.3 Listing of ~~Accepted~~ Crypto-assets (continued)

~~(g) The geographic distribution of the crypto-asset and the relevant trading pairs, if any;~~

~~(h) Whether the crypto-asset has any in-built anonymization functions;~~

~~(i) Whether the crypto- asset has used or was used with any smurfing technology, mixers or has been traded or traded on any Dark-net marketplace/s;~~

~~(j) Whether the crypto-asset is or has been traded on any sidechains;~~

~~(k) Whether the crypto-asset has any inbuilt mechanism which caters for settlement failure, such as resolution mechanisms;~~

~~(l) Other crypto-asset exchanges on which the crypto-asset is traded, if any;~~

~~(m) Security: consideration of whether the specific crypto-asset is able to withstand, adapt, respond to, cyber security vulnerabilities, including size, testing, maturity, and ability to allow the appropriate safeguarding of secure private keys; Traceability/Monitoring: 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;~~

~~(n) Traceability/Monitoring: 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.~~

~~(o) Connectivity: whether there are (other) entities that support the crypto asset; the jurisdictions of these entities and whether these entities are suitably regulated;~~

~~(p) Market demand / volatility: the sufficiency, depth and breadth of client demand, the proportion of the crypto-asset that is in free float and;~~

~~(q) Type of Distributed Ledger: whether there are issues relating to the security and/or usability of a distributed ledger technology used for the purposes of the crypto-asset; whether the crypto-asset leverages an existing distributed ledger for network and other synergies; whether this is a new distributed ledger that has been demonstrably stress tested;~~

~~(r) Innovation / efficiency: for example, whether the crypto-asset helps to solve a fundamental problem, addresses an unmet market need or creates value for network participants; and~~

~~(s) Practical application/functionality: whether the crypto-asset possesses functionalities for real world practical application which is quantifiable.~~

~~CR A-4.3.4 Applicants applying for a license must submit the details of each crypto-asset that is proposed to be used for their regulated crypto-asset service. The use of these crypto-asset must be approved as part of the formal application process.~~

~~CRA-4.3.5 An accepted crypto-asset may be deemed suitable for regulated crypto-asset services by more than one licensee, subject to each licensee satisfying the CBB that it can suitably use each specific accepted crypto-asset.~~

MODULE	CRA: Crypto-asset
CHAPTER	CRA-4 Business Standards and Ongoing Obligations

CRA-4.3 Listing of ~~Accepted~~ Crypto-assets (continued)

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-4.3.8 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 facilitates or may facilitate the obfuscation or concealment of the identity of a customer 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 ~~Accepted~~ Crypto-assets (continued)

CRA-4.3.13 Licensees must ensure that:

(a) its board of directors reviews and independently makes decisions to approve or disapprove each new crypto-asset;

(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 minutes of the board of directors meeting held to approve a crypto-asset, the documents the board of directors 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) its board of directors reviews, at least annually, the crypto-asset listing policy 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 risks to be assessed 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 by a legitimate entity or entities 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);

CRA-4.3 Listing of ~~Accepted~~ Crypto-assets (continued)

and that the process is subject to a strong governance and control framework. Licensees must consider the following factors while undertaking the due diligence:

(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;

(viii) Crypto-asset exchanges on which the crypto-asset is traded.

(b) 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 customer on-boarding and customer support based on reasonable forecasts considering the overall operations of the licensee;

(c) Risks associated with any technology or systems enhancements or modification requirements necessary to ensure timely adoption or listing of any new crypto-asset;

(d) Risks related to cybersecurity: Whether the crypto-asset shall be able to withstand, adapt, respond to, cyber security vulnerabilities, including size, testing, maturity, and ability to allow the appropriate safeguarding of secure private keys;

(e) 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.

CRA-4.3 Listing of ~~Accepted~~ Crypto-assets (continued)

(f) 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;
(g) 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;
(h) 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;
(i) 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
(j) Type of distributed ledger: whether there are issues relating to the security and/or usability of a distributed ledger technology used for the purposes of the crypto-asset; whether the crypto-asset leverages an existing distributed ledger for network and other synergies; whether this 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 not be less than 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 customers and counterparties in the case of such de-listing.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-4 Business Standards and Ongoing Obligations

CRA-4.3 Listing of ~~Accepted~~ Crypto-assets (continued)

Disclosure

CRA-4.3.16 **Licensees must make adequate disclosures 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 detail 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 Bahrain and/or it may affect the legitimate interest of investors, it may, at its sole discretion, instruct licensees to delist the crypto-asset. In such an event, licensees shall remain responsible for orderly settlement and any liability arising due to the delisting of the crypto-asset and obligations arising due to the delisting of the crypto-asset must be resolved by the licensee in a manner that addresses investors concerns appropriately.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-4 Business Standards and Ongoing Obligations

CRA-4.4 Eligible Investors

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 that applicants applying to be registered as clients must be:

(a) a legal person incorporated either in the Kingdom of Bahrain or in an overseas jurisdiction under the law of its place of incorporation; or

(b) a natural person ~~above~~ who is 21 years of age or above. However, licensees may register applicants who have attained the age of 18 but are below 21 years with stringent trading limits. Where a licensee register clients between the age of 18-21, it must undertake proper risk assessment and implement appropriate level of control measures, which must include, amongst others, lower trading limits and restrictions on the type of products and services to be provided.

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 ~~While registering an applicant, licensees must seek the bank account details and a recent bank statement (not older than 2 months).~~

Prior to commencement of business transactions, licensees must:

(a) seek and register bank accounts detail and other types of accounts details to be used for receipt or transfer of fiat funds (such as 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 conduct any deposits and withdrawals of fiat funds through any other 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 Eligible Investors (continued)

CRA-4.4.7 ~~While registering an applicant, licensees must take all reasonable steps to establish the true and full identity of each of the client, and of the client's financial situation, investment experience, and investment objectives.~~ Where an applicant's IP address is masked (for example, where access is via a virtual private network), 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 Section MIR-4.7 of Module MIR except for MIR-4.7.14.**

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 ~~accepted~~ crypto-assets and money (client money) belonging to them which are held or controlled by the licensee, a licensee must hold clients' money and/or to ~~accepted~~ crypto-assets in specially created and segregated accounts. These accounts must be identified separately from any accounts used to hold money and/or to ~~accepted~~ 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 that 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 Licensees must hold client money in a separate client bank account as specified in Paragraphs MIR-4.7.10, MIR-4.7.11, MIR-4.7.12 and MIR-4.7.13. client bank accounts must be opened with retail banks licensed to do business in the Kingdom of Bahrain.**~~

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 properly handle and safeguard client money. The arrangement to handle and safeguard client money, must include but is not limited to the following:**

(a) Establishing one or more client bank accounts with a retail bank licensed to do business 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;

CRA-4.5 Client Protection (continued)

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 client's written instructions, including standing authorities or one-off directions.

CRA-4.5.5B 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 clients' money.

CRA-4.5.7 Licensees must also reconcile, at least on a monthly basis, the total of the balances on all clients' 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 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) the nature of crypto-assets may lead to an increased risk of fraud or cyber-attacks;

(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 and valuations 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; ~~and~~
(g) such other disclosures as are customarily given in connection with the opening of client accounts;
(h) how the licensee will compensate its clients in the event of a cyber hack or other incident involving loss of crypto-assets belonging to client caused on account of an operational failure or error caused by the licensee; and
(i) the rights and entitlements of a client when events such as, but not limited to, forks and airdrops occur.

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 an ~~accepted~~ 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 ~~accepted~~ 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 A licensee must make available to the CBB, upon request, the form of the confirmation note it is required to provide to clients in accordance with Rule CRA- 4.5.12.

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
(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 wants to make his/her account active after 12 continuous months or thereafter, the licensee must ensure that clients submit 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, the account can be made active and transactions can take place.

Client Agreements and Statements

CRA-4.5.15 Licensees must not carry out a regulated crypto-asset service where this involves service to a client as mentioned under Paragraph CRA-1.1.6 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, and if it is a branch of an overseas crypto-asset exchanger, the name and address of the ultimate holding company;

(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.

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;
(i) details of any restrictions, such as a block order from the court or other competent authority; and
(j) where client assets are held under custody arrangement with a third-party custodian, the name and address of the third-party custodian.

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, and the statement of account 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 ensure that it has obtained consent from its clients and put in place adequate operational safeguards, to prevent unauthorised access, if any confirmation note, statement of account or other statements required to be provided to a client is provided by electronic mode (email) or by accessing its website. Licensees must provide the client with the various alternatives available for receiving confirmation note, statement of account or other statements and allow the client to decide on the most suitable mode.**

CRA-4.5 Client Protection (continued)

CRA-4.5.22 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:

(i) there are no transactions; and
(ii) the account balance (funds) is nil; and
(iii) the balance of crypto-assets held on behalf of the client is nil.

No Restriction on Withdrawal of Client Assets

CRA-4.5.23 Where a client requests for withdrawal of client assets, a licensee must not impose restriction on withdrawal of the client assets held under its control, unless there are specific reasons to impose restriction on withdrawals. Where a licensee imposes restriction on withdrawal of client assets, it must inform the client and the CBB, in writing, the reason for imposition of restriction on withdrawal of the client assets.

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 the legend 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 In all advertising and marketing materials, licensees must comply with all disclosure requirements under CBB Law, Rules and regulations.

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 and trading rules 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 personal information to third parties, including regulators;
(k) client's right to prior notice of any change in the licensee's rules, procedures or policies;
(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 or regulation;
(b) All documentation concerning promotions is in a language that customers can fully understand;
(c) Customers to whom promotions are directed must have equal opportunity in terms of access to, and treatment;
(d) The communication concerning promotions must be clear, concise, truthful, unambiguous and complete to enable customers 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 fairly and timely resolve complaints.

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;
(b) a statement that the complainant may also bring his or her complaint to the attention of the CBB; and
(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.

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) Recurring systems failures are identified, investigated and remedied;
(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; ~~and~~
(e) Relevant employees are aware of the licensee's internal complaint handling procedures and 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 in writing to a customer complaint within 4 weeks of receiving the complaint, explaining their position and how they propose to deal with the complaint.~~

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. If a licensee fails to respond to a client complaint as above, the licensee will be liable for appropriate enforcement actions as per the Market Surveillance, Investigation and Enforcement (MIE) Module, including financial penalties.

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 Should the customer that filed a complaint not be satisfied with the response received as per Paragraph CRA-4.7.7, he can forward the complaint to the Compliance Directorate 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 ~~Office~~ Unit at the CBB, a quarterly report summarising the following:

(a) The number of complaints received;
(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 ~~office~~ 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) that covers loss of money or loss or damage to any other asset or property belonging to the licensee or which is in the care, custody or control of the licensee or for which the licensee is responsible.

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) includes 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 **Licensees must not enter into or make a claim under a contract of insurance that is intended to, or has the effect of, indemnifying them from the financial penalties.**

CRA-4.8.6 The requirement to maintain professional indemnity coverage will normally be met by the licensee concerned 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. Similarly, a licensee operating a branch may provide evidence of professional indemnity coverage maintained by their head office, providing that the coverage of the professional indemnity extends to the operations of the branch operating in Bahrain.

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 **Unless otherwise agreed in writing with the CBB, 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 A licensee must, in connection with its regulated crypto-asset service, maintain books and records as set out in Rule MIR-4.6.1, MIR-4.6.2, MIR-4.6.3 and MIR-4.6.6 of Module MIR.

Obligation to Maintain Confidentiality

CRA-4.9.2 A licensee must maintain the confidentiality of all client information as set out in Section MIR-4.12 of Module MIR.

Records of Telephone conversations and Electronic Communications

CRA-4.9.3 A licensee must comply with the requirements of maintaining records of telephone conversations and electronic communications as set out in Rule MIR-4.14.2.

CRA-4.10 Matters Requiring Approval of CBB

CRA-4.10.1 **A licensee must comply with the following Rules of Module MIR, when there is a change of shareholding held by substantial shareholders, or a transfer of business or substantially all its assets or liabilities:**

(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 subject to Paragraph CRA-4.10.3 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 and these Rules issued hereunder, 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;

(d) the method of determining the remuneration of the relevant persons involved in the compliance function must not compromise their objectivity and must not be likely to do so.

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 With respect to Paragraph CRA-4.11.4(b), the appointment of an individual as Compliance Officer is subject to CBB's prior approval. The CBB may, at its discretion, may allow the compliance office 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 Office without compromising on supervisory objectives.

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

~~*Listing and Trading of Crypto-assets*~~

CRA-4.12.1 ~~A licensed crypto-asset exchange must not permit the trading of accepted crypto-assets without the prior written approval of the CBB.~~

CRA-4.12.2 ~~An application for the listing of an accepted crypto-asset must be accompanied by the required information for approval at least 30 days prior to commencement of the intended listing.~~

CRA-4.12.3 ~~For the purposes of Paragraph CRA-4.12.2, a licensed crypto-asset exchange, as a minimum, must provide information pertaining to the crypto-asset as specified under Paragraph CRA-4.3.3.~~

Suspension of trading and delisting

CRA-4.12.4 **A licensed crypto-asset exchange must not delist or suspend the trading of ~~accepted~~ crypto-assets without the prior written approval of the CBB.**

CRA-4.12.5 **Without prejudice to the right of the CBB to demand suspension or delisting of a~~n~~ ~~accepted~~ crypto-asset from trading, a licensed crypto-asset exchange must suspend or delist from trading a~~n~~ ~~accepted~~ 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 suspend~~s~~ or delist~~s~~ from trading a~~n~~ ~~accepted~~ crypto-asset, it must by way of a public announcement inform the clients' regarding the date of suspension or delisting of the ~~accepted~~ crypto-asset.**

CRA-4.12.7 Where a llicensed crypto-asset exchange has suspended or delisted an ~~accepted~~ 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 ~~accepted~~ 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 ~~accepted~~ 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 ~~accepted~~ 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 ~~accepted~~ 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 ~~accepted~~ crypto-assets; and
(c) any other information relating to ~~accepted~~ 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 ~~accepted~~ 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 ~~accepted~~ 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 ~~accepted~~ 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.

Reporting of Suspicious Transactions

CRA-4.12.16 A licensed crypto-asset exchange must immediately report to the CBB any transaction which breaches or which the licensed crypto-asset exchange suspects to have breached these Rules, particularly with respect to Chapter-13 (Prevention of Market Abuse and Manipulation).

Exchange Systems

~~**CRA-4.12.17** A licensed crypto-asset exchange must have in place effective systems, procedures and arrangements to ensure its trading 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 its services if there is any failure of its trading 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~~n~~ ~~accepted~~ 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. Such information must be made available to the CBB upon request.

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 ~~accepted~~ 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 ~~accepted~~ 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 and resolution systems which cater for such failures. Such systems should be clearly documented in the licensed crypto-asset exchange's bye-laws.**

CRA-4.12.32 **A licensed crypto-asset exchange must establish a system that monitors settlement fails of transactions in ~~accepted~~ crypto-assets. It must provide regular reports to the CBB, as to the number and details of settlement fails 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 ~~accepted~~ crypto-assets being traded on its platform is being traded in a fair, orderly and efficient manner. Such bye-laws, 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 ~~accepted~~ 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) disciplinary action 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)

Disciplinary Action

CRA-4.12.37 Where a licensed crypto-asset exchange has taken any disciplinary action against any of its clients, including the suspension of the client from trading, the blacklisting or expelling of a client or any other disciplinary action, in respect of a breach of its directives or 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 disciplinary action taken by the licensed crypto-asset exchange; and
(d) the reasons for taking that disciplinary action.

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 ~~accepted~~ crypto-asset funds: Systems and controls to mitigate the risk of misuse of crypto currencies, setting out how:

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

(viii) the destination of ~~accepted~~ 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 ~~accepted~~ crypto-assets; and

(iv) risk of financial crime.

CRA-5.1.3 The CBB may grant exemption 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 the integrity of the market and/or interest of clients will not be compromised.

System Resilience

CRA-5.1.4 **Licensees must have in place effective systems, procedures and arrangements to ensure its IT system 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 its services if there is any failure of its trading systems.**

CRA-5.1 General Requirements (continued)

CRA-5.1.5 Licensees must continuously monitor the utilisation of its 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.

~~*IT System Audit*~~

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

CRA-5.2.7 ~~Licensees must conduct test of their IT infrastructures and core systems to verify the robustness of the security control measure that is in place to prevent security breaches. These tests, among others, must include penetration testing and vulnerability assessment of the IT infrastructure. The test must be undertaken by an external independent party that have security professionals, such as ethical hackers, and not by employees of the licensee or entities associated with the licensee.~~

CRA-5.2.8 ~~The testing of IT infrastructure and core system including penetration testing and vulnerability assessment referred to in Paragraph CRA-5.2.7 must be conducted each year in June and December, and the assessment report, along with the steps taken to mitigate the risks must be provided to the CBB within two months from the end of the reporting period.~~

~~CRA-5.2.9~~ ~~Licensees must maintain the assessment report along with the steps taken to mitigate the risks referred to in Paragraph CRA-5.2.8 for a period of 5 years.~~

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. A strong security policy 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 ~~accepted~~ 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. (see also CRA-4.1.2 and CRA-4.1.3).**

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 **~~Accepted~~ Crypto assets ~~currencies~~ that do not need to be immediately available ~~should~~ must be held off line, in a 'cold wallet' (refer to CRA-8.1.~~97~~) ~~to the extent feasible~~. ~~Below is a non-exhaustive list of some of the measures that licensees should consider.~~**

Password protection and encryption

CRA-5.4.4 **Both hot and cold wallets ~~should~~ must be password protected and encrypted. The key storage file that is held on the online or offline device ~~should~~ 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 ~~should consider~~ must ~~the~~ use ~~of~~ multi-signature wallets (e.g., where multiple private keys are associated with a given public key and a subset of these private keys, ~~sometimes~~ held by different parties, are required to authorise transactions). Noting that there is no way to recover stolen or lost private keys unless a copy of that key has been made, multi-signature wallets ~~may~~ offer more security because a user can still gain access to its crypto-assets when two or more Private Keys remain available. (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.

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 must be taken not to infect the air-gapped device with malware

CRA-5.4 Cryptographic Keys and Wallet Storage (continued)

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. These 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 key (if seed are not used) are generated in a non-deterministic manner which ensures randomness and thus 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;

(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;

CRA-5.4 Cryptographic Keys and Wallet Storage (continued)

(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 needs to 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 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-5.4.12 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. Where a licensee maintains a physical copy of the seed and private key is must maintained in Bahrain.~~

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 and 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 done 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-5.6.4 **Licensees must inform the CBB as soon as possible, but not later than one hour, upon occurrence or detection of any system outage, whether internal or external, that compromises customer information or disrupts critical services that affect operations.**

CRA-5.6.5 **Following the submission of preliminary information referred to in Paragraph CRA-5.6.4, the licensee must submit to CBB a detailed report within 5 days of the occurrence of the unplanned outage. 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 customers, and all measures taken by the licensee to 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-5.6.6 With regards to the submission requirement mentioned in Paragraph CRA-5.6.5, the licensee should submit the report with as much information as possible even if all the details have not been obtained yet.

CRA-5.7 Board oversight, Management of Staff and Decision Making

CRA-5.7.1 Licensees must implement processes and procedures concerning decision making and access to sensitive information and security systems.

CRA-5.7.2 A clear audit log of decision making must be kept. Staff with decision-making responsibilities must have the adequate expertise, particularly from a technological standpoint, to make such decisions.

CRA-5.7.3 Protective measures must be implemented to restrict access to critical and/or sensitive data to key staff only. This includes both digital and physical access. Licensees must have processes and procedures to track and monitor access to all network resources. Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimising the impact of a data compromise. The maintenance of logs allows thorough tracking, alerting, and analysis when issues occur.

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 systems 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. At the broader level, the Cyber security 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 CFO / 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. The board must establish clear ownership, decision-making and management accountability for risks associated with cyber-attacks and related risk management and recovery processes.**

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

(a) ensure that the licensee's policies 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 ensure that such policies and procedures are periodically reviewed and improved, 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) ensure that the management continues to promote awareness on cyber resilience at all levels within the entity;
(f) 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

CRA-5.8 Cyber Security (continued)

(g) 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 entity; 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-5.8.4B The 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. The cyber security staff are adequate to manage the licensee's cyber security risks and facilitate the performance and continuous improvement of all relevant cyber security controls;
d. It provides and requires cyber security staff 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 Cyber Security (continued)

CRA-5.8.4C With respect to Paragraph CRA5.8.4B(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 of the policy 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. In other words, there should be little (if any) overlap in the classification definitions. The owner of data (i.e. the relevant business function) should be involved in such classification.

Cyber Security Strategy

CRA-5.8.4D **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-4.8.4E 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 reference to support the licensee's cyber security strategy and cyber security policy.

CRA-5.8 Cyber Security (continued)

Cyber Security Risk Policy

CRA-5.8.5 Licensees must implement a written cyber security risk policy setting forth the licensee's Board approved policies and related procedures that are approved by senior management, for the protection of its electronic systems and clients data stored on those systems, which 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) Clear description of the risk tolerance in relation to cyber security risk that is acceptable to the licensee such as, occurrence and severity of cyber security breaches, the maximum service downtime, recovery time objectives, minimum level of system and services availability, potential negative media publicity, potential regulatory and financial impact or a combination of other measures;~~ A statement of the licensee's overall cyber risk tolerance aligned with the licensee's business strategy must consider service downtime, recovery time objectives and occurrence/severity of cyber security breaches. The statement must also consider the impact on customers, 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;

(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

CRA-5.8 Cyber Security (continued)

(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.

Cyber Security Risk Measure

CRA-5.8.6 A licensee must ensure that comprehensive strategies and measures are in place to manage cyber security risk including prevention, detection and recovery measures.

CRA-5.8.7 Notwithstanding that the operation or maintenance of information assets, systems and network are outsourced to a third-party service provider, the licensee remains responsible for ensuring compliance with the requirements specified in this Module.

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 Cyber Security (continued)

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 anti-malware programs~~mc~~ 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; ~~Build firewalls to reduce weak points through which attacker can gain access to a licensee's network~~;

(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; ~~and~~

(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);

(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 Cyber Security (continued)

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. to Controls or solutions to secure, control, manage and monitor privileged access to critical assets, (e.g. Privileged Access Management (PAM))
c. 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
d. 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:**

- **SPF "Sender Policy Framework";**
- **DKIM "Domain Keys Identified Mail"; and**
- **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 customers to prevent abuse by third parties. Licensees must not utilise third-party email provider domains for communication with customers. The email domains must comply with the requirements of Paragraph OM-5.8.11B with respect to SPF, DKIM and DMARC.**

CRA-5.8.11E For the purpose of Paragraph CRA-5.8.11D, branches of foreign entities and 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 customers to receive emails from third-party service providers for specific services offered by such third-parties provided the customers 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 Cyber Security (continued)

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

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

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

(c) Implement measures to allow customers 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 customer action on the licensee's website/app;

ii. communication with customer such as a phone call informing the customer 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 customer with the link;

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

(d) Create customer awareness campaigns to educate their customers on the risk of fraud related to links they receive in SMS, short messages and emails with clear instructions to customers 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 customer request or action. Licensees may also train their customers by sending fake phishing messages.

CRA-5.8.12 A licensee must ensure that the board, management, employees and third parties with whom the licensee deal with undergo appropriate training on a regular basis to enhance their awareness and preparedness to deal with a wide range of cyber security risks, incidents and scenarios.

CRA-5 .8.13 A licensee must evaluate improvement in the level of awareness and preparedness to deal with cyber security risk to ensure the effectiveness of training programmes implemented.

CRA-5.8 Cyber Security (continued)

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 if available; 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 are 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 CBB may require additional third-party security reviews to be performed as needed.

CRA-5.8.13I **The penetration test and the vulnerability assessment by an independent third party, referred to in Paragraph CRA-5.8.13G(e) and, must be conducted each year in June and December 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, i.e. for a June test, the report must be submitted at the latest by 31st August and for a December test, by 28th February. 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~~ ~~**In addition to implementing preventive measures, a licensee must continuously monitor for any cyber security incidents and breaches within its systems and network.**~~

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-5.8.14C 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-5.8.14D **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 customers. Such responsibilities must include log correlation, anomaly detection and maintaining the licensee's asset inventory and network diagrams.**

CRA-5.8.14E **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-5.8.14F 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 Cyber Security (continued)

CRA-5.8.14G **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 CBB.**

CRA-5.8.14H 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:

- **Incident Owner:** An individual that 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.
- **Spokesperson:** An individual, from External Communications Unit or another suitable department, that 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.
- **Record Keeper:** An individual that 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 serves as an accurate source of reference for after-action reviews to improve future cyber incident detection and response activities.

CRA-5.8.14I 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-5.8.14J 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 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 Cyber Security (continued)

CRA-5.8.14K 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 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 customers, data leakage, unavailability of data, data destruction/corruption, tarnishing of reputation)
(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 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-5.8.14L Licensees should determine the effects of the cyber incident on customers and to the wider financial system as a whole and report the results of such an assessment to CBB if it is determined that the cyber incident may have a systemic impact.

CRA-5.8.14M Licensees should establish metrics to measure the impact of a cyber incident and to report to management the performance of response activities. Examples include:

1. Metrics to measure impact of a cyber incident
   (a) Duration of unavailability of critical functions and services
   (b) Number of stolen records or affected accounts
   (c) Volume of customers impacted
   (d) Amount of lost revenue due to business downtime, including both existing and future business opportunities
   (e) Percentage of service level agreements breached
2. Performance metrics for incident management
   (a) Volume of incidents detected and responded via automation
   (b) Dwell time (i.e. the duration a threat actor has undetected access until completely removed)
   (c) Recovery Point objectives (RPO) and recovery time objectives (RTO) satisfied

CRA-5.8 Cyber Security (continued)

CRA-5.8.15 ~~A licensee must ensure timely detection of and response to cyber security breaches within a clearly defined escalation and decision-making processes to ensure that any adverse effect of a cyber security incident is properly managed and initiate recovery action quickly.~~

CRA-5.8.16 ~~To ensure sufficient preparedness in responding to cyber security incidents detected, the licensees must:~~

~~(a) identify scenarios of cyber security risk that the licensee is most likely to be exposed to;~~

~~(b) consider incidents in the crypto-asset markets and the broader financial services industry;~~

~~(c) assess the likely impact of these incidents to the licensee; and~~

(d) ~~identify appropriate response plan and communication strategies that must be undertaken.~~

CRA-5.8.17 ~~A licensee must regularly test, review and update the identified cyber security risk scenarios and 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.~~

CRA-5.8.18 ~~A licensee must ensure that cyber security breaches detected are escalated to an incidence 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.~~

CRA-5.8.19 ~~A licensee must submit a preliminary report to the CBB on any detection of a cyber security incident which may or have had an impact on the information assets or systems of the licensee, on the day of the occurrence of the incident. The preliminary report submitted to the CBB under this Paragraph must be made in accordance with the reporting template as provided in Appendix 1.~~

CRA-5.8.19A ~~A licensee, following submission of the preliminary report on detection of a cyber security incident referred to in Paragraph CRA-5.8.19, must submit to the CBB a comprehensive report within 5 working days of the occurrence of the cyber security incident. The comprehensive report must include all relevant details including the root cause analysis of the cyber security incident and measures taken by the licensee to ensure that similar events do not recur.~~

CRA-5.8 Cyber Security (continued)

Recovery

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

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 level of services during the downtime and determine how much time the licensee will require to return to full service and operations.**

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; and
d) Operational aspects and delivery of key products and services.

CRA-5.8.20C **Licensees must define a program for recovery activities for 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 in 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, customers 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 Cyber Security (continued)

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 customers.

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 "table top" 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-5.8.21 ~~**A licensee 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 level of services during the downtime and determine how much time the entity will require to return to full service and operations.**~~

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]**

CRA-5.8 Cyber Security (continued)

IT System Audit

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

CRA-5.8.25A ~~A licensee must conduct a periodic assessment of cyber security threats for the purpose of analysing and assessing cyber security threats, the licensee must take into account the factors detailed below:~~

~~(a) Surveys and audit findings, and all current information that could be indicative of weaknesses in the relevant controls;~~

~~(b) Collection and analysis of external data that could be indicative of potential vulnerabilities or lead to the detection of risk exposures that were not identified in the past;~~

~~(c) Collection and analysis of data regarding cyber security incidents within the licensee;~~

~~(d) Mapping of business processes for the purpose of exposing specific risks, interdependencies between risks, and areas of weakness in controls or risk management;~~

~~(e) Use of metrics for the purpose of quantifying the exposure to cyber security risks, use of qualitative and/or quantitative assessment indicators, in a manner that should make it possible to monitor changes in these values from time to time;~~

~~(f) Use of Key Risk Indicators (KRIs) and Key Process Indicators (KPIs), in order to provide insights on the status of control mechanisms and the cyber security program;~~

~~(g) Analysis of scenarios, in licensee with business line managers and risk managers in order to detect potential incidence of risk materialization, to assess their potential impact, and to enhance the ability to detect and respond to those incidents.~~

Application Security

CRA-5.8.26 ~~The cyber security policy must, at minimum, include written procedures, guidelines, and standards reasonably designed to ensure the security of all applications utilized by the licensee. All such procedures, guidelines, and standards must be reviewed, assessed, and updated by the licensee's CISO at least annually.~~

CRA-5.8 Cyber Security (continued)

Personnel and Intelligence

CRA-5.8.27 ~~A licensee must:~~
~~(a) employ cyber security staff adequate to manage the licensee's cyber security risks and to perform the core cyber security functions;~~
~~(b) provide and require cyber security staff to attend regular cyber security update and training sessions; and~~
~~(c) require key cyber security staff to take steps to stay abreast of changing cyber security threats and countermeasures.~~

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 to analyse the insured's legal response obligations;
(b) Claim expenses such as costs of defending lawsuits, judgments and settlements, and costs of responding to regulatory investigations; and
(c) Policy also provides coverage for a variety of torts, including invasion of privacy or copyright infringement. First-party coverages may include lost 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 insured.

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 Cyber Security (continued)

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 CBB

CRA-5.8.33 Upon occurrence or detection of any cyber security incident, whether internal or external, that compromises customer 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 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-5.8.34 Following the submission referred to in Paragraph CRA 5.8.33, the licensee must submit to 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 customers, 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 must take responsibility 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 of Section 2.6. 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 firm'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 (for ~~accepted~~ crypto-assets);
(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;
(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 allow 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 and regularly reviewed by the Board of Directors 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 and regularly reviewed by the Board of Directors 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 appropriate to the nature, scale and complexity of its activities. This policy must be approved and regularly reviewed by the Board of Directors 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 and regularly reviewed by the Board of Directors 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 others:**

(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 is 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-6.5.6 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;

(c) 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;

(d) 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;

(e) 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

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

CRA- 6.5.7 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 -6.5.8 Licensees must provide relevant training to all employees responsible for implementing the business continuity and disaster recovery plan regarding their roles and responsibilities.

CRA-6.5.9 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-6.5.10 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:

1. The head office/regional office declares its ultimate responsibility of ensuring that adequate control measures are in place; and
2. 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:**

1. **Compliance;**
2. **AML/CFT;**
3. **Financial control;**
4. **Risk management; and**
5. **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 (4), subject to CBB's prior approval.

CRA-6.6 Outsourcing Arrangements (continued)

CRA-6.6.7 Licensees must comply with the following requirements:

1. 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.
2. Post notification to the CBB, within 5 working days from entering into the outsourcing arrangement, 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.
3. 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.
4. 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.
5. Licensees must designate an approved person to act as coordinator for monitoring and assessing the outsourced arrangement.
6. 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.
7. 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 (4), 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-6.6.7 (1), 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.

MODULE	CRA: Crypto-asset
CHAPTER	~~CRA-7 Anti-Money Laundering & Combating of Financial Crime~~

~~CRA-7.1 General Requirements~~ [This Chapter was deleted in XX 2022]

~~CRA-7.1.1 Licensees must ensure that all of its clients maintain a bank account either with a licensed retail bank in Bahrain or with an overseas retail bank licensed and supervised by a regulator acceptable to the CBB.~~

~~CRA-7.1.1A Regulated crypto-asset services present money laundering and terror financing risks and other crime risks that must be identified and mitigated. Accordingly, licensees must implement and comply with the full set of obligations as specified in this Section and Module AML.~~

~~CRA-7.1.2 [This Paragraph was deleted in January 2020].~~

~~CRA-7.1.3 Licensees must conduct enhanced customer due diligence (EDD) as set out in Section AML-1.8 of Module AML on all customers and counterparties, including for introduced business when the licensee establishes business relationship; and when the licensee have any suspicion of Money Laundering/Terror Financing. Licensees must not apply simplified customer due diligence measures for on boarding of customers.~~

~~CRA-7.1.4 Licensees must not register charitable funds, religious, sporting, social, cooperative and professional and other societies register as clients or establish business relations with such entities. Therefore, licensees are not subject to the EDD and other requirements specified for charities, clubs and other societies stipulated in Section AML-1.6 of Module AML.~~

~~CRA-7.1.5 Licensees must comply with the customer due diligence and transaction records as stipulated in AML-6 (Record Keeping) of Module AML.~~

CRA-8.1 General Requirements

CRA-8.1.1 The Rules in this Section apply to licensees that undertakes safeguarding, storing, holding or maintaining custody of ~~accepted~~ crypto-assets as specified in Paragraph CRA-1.1.6(e).

CRA-8.1.2 A licensee that undertakes safeguarding, storing, holding or maintaining custody of ~~accepted~~ crypto-assets, on behalf of their clients, is considered a "crypto-asset custodian", and must comply with the requirements of Chapter 8 at all times.

CRA-8.1.3 A licensee which undertakes safeguarding, storing, holding or maintaining custody of ~~accepted~~ crypto-assets must have systems and controls in place to:

(a) Ensure the proper safeguarding of ~~accepted~~ crypto-assets;
(b) Ensure that such safe custody of ~~accepted~~ crypto-assets is identifiable and secure at all times; ~~and~~
(c) Be able to evidence compliance with the requirements of Section 7 to its external auditors and the CBB; and
(d) Ensure protection against the risk of loss, theft or hacking.

CRA-8.1.4 As part of these protections, the custody Rules require a licensee to take appropriate steps to protect ~~accepted~~ crypto-assets for which it is responsible.

CRA-8.1.5 To the extent a licensee stores, holds, or maintains custody or control of ~~accepted~~ crypto-asset on behalf of a client, such licensee must hold ~~accepted~~ 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 ~~accepted~~ 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 ~~accepted~~ 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, amongst

CRA-8.1 General Requirements (continued)

others, having separate staffing arrangement to undertake crypto-asset custody activity, which does not have any conflicting responsibilities within the licensee.

CRA-8.1.8 A licensee that maintains custody or control of crypto-assets, must ensure that transfer of crypto-assets out of a client's account is undertaken only upon the client's express instruction, and not on its own initiative or discretion.

CRA-8.1.9 A licensee that maintains custody or control of crypto-assets on behalf of a client must store, at a minimum, 95% of client's crypto-assets in cold wallets to minimise exposure to losses arising from a compromise or hacking. The requirement to hold 95% 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-8.1.10 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-8.1.11 A licensee that maintains custody or control of crypto-assets must not, at any time, permit arrangements whereby just a sole party or signatory is able to completely authorise the movement, transfer or withdrawal of 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-8.1.12 A licensee must ensure that crypto-assets held under custody arrangement are properly safeguarded from conversion or inappropriate use by any person, including but not limited to implementing multi-signature arrangements (refer CRA-5.4.5).

CRA-8.1.13 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.

CRA-8.1 General Requirements (continued)

Other Requirements

CRA-8.1.14 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-8.1.15 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 it knows or suspects that the crypto assets it is holding under custody on behalf for clients has been compromised, such as in the event of a hacking attack, theft or fraud. Such policies and procedures must detail the specific steps the licensee will take to protect clients 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-8.1.16 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-8.1.17 Licensees must ensure that changes in the underlying protocol of an 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-8.1.18 Licensees 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 General Requirements (continued)

CRA-8.1.19 Where the underlying protocol of an 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), licensees 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. Licensees maintain transparent lines of communication with their clients on how licensees are managing clients crypto-asset holdings in such a scenario.

CRA-8.1.20 In the case of a hard fork, licensees 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 its 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 maintaining custody of ~~accepted~~ 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 ~~accepted~~ 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 ~~accepted~~ 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 ~~accepted~~ 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 ~~accepted~~ crypto-assets. Such licensees only provide the platform for clients to buy and sell ~~accepted~~ 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 ~~accepted~~ 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 ~~accepted~~ 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 Rule 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 firm 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 ~~accepted~~ crypto-assets;
(c) An appropriate legal opinion as to the protection of ~~accepted~~ 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 Module MIR.**

CRA-8.2 Custodial Arrangements

CRA-8.2.6 **A licensee that safeguards, stores, holds or maintains custody of ~~accepted~~ 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 **A licensee must be able to demonstrate to the CBB's satisfaction the grounds upon which the licensee considers the third party crypto-asset custodian to be suitable to hold ~~accepted~~ crypto-assets.**

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 ~~accepted~~ crypto-assets as being a material risk given that the burden of protecting and safeguarding ~~accepted~~ crypto-assets falls wholly upon clients, and that the ~~accepted~~ crypto-assets face the constant risk of being stolen by malicious actors. As such, licensees requiring clients to self-custodise ~~accepted~~ 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 For the purposes of Paragraph CRA-8.2.2(c) and Paragraph CRA-8.2.8, the CBB will give consideration to the quality of disclosure made to clients while assessing application from licensees proposing to require client to self-custodise their ~~accepted~~ crypto-assets.

CRA-8.3 Crypto Wallets

CRA-8.3.1 **Licensees must put in place necessary Rules and regulations for crypto-asset wallets.**

CRA-8.3.2 For the purposes of Paragraph CRA-8.3.1, licensees should consider, at the minimum, the following two types of crypto-asset wallets:

(a) Custodial Wallet: the custodial wallet provider holds ~~accepted~~ 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 holds ~~accepted~~ 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.

(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 currencies – 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-8.3.4 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 ~~accepted~~ 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 his ~~accepted~~ crypto-assets.

CRA-8.3 Crypto Wallets (continued)

CRA-8.3.5 Licensees that outsource their crypto-asset wallets to a third party are considered as "arranging custody" and must comply with the requirements of this Chapter.

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 implement appropriate storage solutions to ensure the secure storage of crypto-assets held on behalf of clients. Where a licensee maintains custody of crypto-assets with a third-party crypto-asset custodian, the licensee must ensure that the appointed third-party crypto-asset custodian implements the same measures in compliance with the requirements of this Module and. In particular, the licensee must keep, and where applicable, must ensure that its third-party crypto-asset custodian keeps, the wallet storage technology up-to-date and in line with international best practices or standards. 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 virtual 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 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 and its appointed third party crypto-asset custodian, if any, 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 should be clear processes in place to evaluate the potential impact and risks of these developments as well as 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)

(c) have clear processes in place to minimise the risks involved with 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;

(d) 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

(e) 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-8.4 Reconciliation, Client Reporting and Record Keeping

Reconciliation

CRA-8.4.1 A licensee must at least every calendar month:

(a) perform reconciliation of its record of safe custody ~~accepted~~ crypto-assets held with third party crypto-asset custodians with monthly statements received from those third party crypto-asset custodians;

(b) ~~count~~ aggregate all safe custody ~~accepted~~ crypto-assets ~~physically~~ held by the licensee, or its ~~nominee company~~ third party custodian, and reconcile the result ~~of that count~~ to the records of the licensee; and

(c) reconcile individual client balances with the licensee's records of safe custody ~~accepted~~ crypto-assets balances held in client accounts.

(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 differences.

Client Reporting

CRA-8.4.2 A licensee which provides crypto-asset custody service (including where the licensee has a third-party crypto-asset custody arrangement) must send a soft copy of the statement to its client at least every calendar month.

CRA-8.4.3 The statement referred to in Paragraph CRA-8.4.2 must include:

(a) a list of that client's safe custody ~~accepted~~ crypto-assets as at the date of reporting; and

(b) details of any client money held by the licensee as at the date of reporting.

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, a licensee must maintain proper records in relation to a client account; these 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 ~~accepted~~ crypto-assets held and movements in each account; and
(g) The date of opening and where applicable, closure.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-9 High Level Controls

CRA-9.1 Corporate Governance

CRA-9.1.1 A licensee must meet ~~the corporate governance principles issued by the Ministry of Industry, Commerce and Tourism as The Corporate Governance Code and~~ the requirements of Chapter HC-10 of Module HC.

CRA-10.1 Reporting Requirements

Reports Prepared by a Licensee

CRA-10.1.1 Licensees must report any actual or attempted fraud incident (however small) to the appropriate authorities (including the CBB) (ref. AML-12.1.4).

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 Office 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 partner 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 report providing the month wise breakup of value of trades undertaken by each client for the reporting quarter. This report must include information about:
  (i) Name and Client ID;
  (ii) Place of residency;
  (iii) Nationality of the client;
  (iv) Crypto-asset type;
  (v) Type of transaction (Buy or Sell);
  (vi) Volume of transaction;
  (vii) Value of transaction including currency; and
  (viii) Value of transaction in BHD
(b) a report about top 20 clients based on the total value traded during the quarter.
(c) 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 Licensees failing to comply with the requirements of Paragraph CRA-10.1.5 or reporting inaccurate information are subject to financial penalties or other enforcement actions.

CRA-10.1 – Reporting Requirements (continued)

Reports Prepared by External Auditors

CRA-10.1.7 **Licensees that hold or control client assets must arrange for their external auditor to report on the licensees' compliance with the requirements contained in Module MIR (ref: MIR-4.7.22 to MIR-4.7.24) and submit the report to the CBB within three months of the licensee's financial year.**

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-10.1.9 **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 Licensees failing to comply with the requirements of Paragraphs CRA-10.1.8 and CRA-10.1.9 are subject to financial penalties or other enforcement actions.

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, it must notify the CBB immediately (ref. CRA-11.3.2).**

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 of the licensee 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 customers;

(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 Except in instances where the CBB has initiated the following actions, 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 to a substantial shareholder of the licensee (whether an administrative receiver or a receiver appointed over particular property); or
g. An application for an interim order against the licensee, a substantial shareholder of the licensee under the Bankruptcy and Composition Law of 1987 or similar legislation in another jurisdiction.

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 Licensees must notify the CBB of the termination of employment of approved persons, including particulars of reasons for the termination and arrangements with regard to replacement (ref. CRA-1.7.9).

CRA-10.2.13 Licensees must immediately notify the CBB when they become aware of any of the events listed in Paragraph MIR-3.6.1 of Module MIR, affecting one of their approved persons.

CRA-10.2 Notification Requirements (continued)

CRA-10.2.14 Licensees must seek prior CBB approval before an approved person may move from one controlled function to another within the same licensee.

CRA-10.2.15 Overseas crypto-asset service licensees must notify the CBB of any new significant ownership in excess of 50% of the issued and paid up capital of the concerned licensee's direct parent undertaking as soon as the licensee becomes aware of the change.

Listing of Crypto-assets

CRA-10.2.16 Licensees must notify the CBB of any new listing of crypto-assets prior to the date of listing.

CRA-10.2.17 Licensees must, on quarterly basis, provide a list of all the crypto-assets listed on its platform. The aforementioned list of crypto-assets must be submitted to the CBB within 10 days from the end of each quarter (CRA-4.3.9).

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 approval from the CBB and give reasonable advance notice 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 approval from the CBB for its intention 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 customers, 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 CBB approval and give reasonable advance notice of a change in its legal status that may, in any way, affect its relationship with or limit its liability to its customers.

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 CBB 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 In accordance with MIR-7.1 of Module MIR, 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 CBB approval and give three months' notice of its intention to undertake business activities in a jurisdiction other than Bahrain prior to commencing that business and where the effect of commencing that business may have a significant impact on:

(a) The licensee's business in Bahrain; or
(b) The capital resources of the licensee.

10.3 Approval Requirements (continued)

CRA-10.3.13 **Rule 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 this information to consider whether or not it should refuse its approval or 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 CBB approval and give reasonable advance notice of its intention 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 to cancel an authorisation for a subsidiary undertaking must obtain the CBB's written approval, before ceasing the activities of the subsidiary.**

Outsourcing Arrangements

CRA-10.3.17 **A licensee must seek prior approval from the CBB for the following:**

(a) Outsourcing of their internal audit function (ref. CRA-6.6.40)

(b) Material intra-group outsourcing (ref. CRA-6.6.37);

(c) Outsourcing other material functions (ref. CRA-6.6); or

(d) Other material outsourcing.

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 from 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.

Dividend Distribution

CRA-10.3.22 Licensees must obtain the CBB's prior written approval to any dividend proposed to be distributed to the shareholders, in accordance with Paragraph CRA-4.10.2.

External Auditor

CRA-10.3.23 A licensee must seek prior approval from the CBB for the appointment or re-appointment of its external auditor (ref. MIR-4.8 of Module MIR).

Approved Persons

CRA-10.3.24 A licensee must seek prior approval from the CBB for the appointment of persons undertaking a controlled function (ref. Article 65 of the CBB Law, MIR-3.1 of Module MIR).

CRA-10.3.25 Licensees must seek prior CBB approval before an approved person may move from one controlled function to another within the same licensee (ref. MIR-3.5.1 of Module MIR).

CRA-10.3 Approval Requirements (continued)

CRA-10.3.26 If a controlled function falls vacant, a licensee making immediate interim arrangements for the controlled function affected, must obtain approval from the CBB (ref. CRA-1.7.9).

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 may reasonably request 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.

Information Requested on Behalf of other Supervisors

CRA-11.1.4 The CBB may ask a licensee to provide it with information at the request of or on behalf of other supervisors to enable them to discharge their functions properly. Those supervisors may include overseas supervisors or government agencies in Bahrain. The CBB may also, without notifying a licensee, pass on to those supervisors or agencies information that it already has in its possession.

CRA-11.2 Access to Premises

CRA-11.2.1 **A licensee must permit representatives of the CBB, or persons appointed for the purpose by the CBB to have access, with or without notice, during reasonable business hours to any of its business premises in relation to the discharge of the CBB's functions under the relevant 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 take reasonable steps to ensure that all information they give to the CBB is:

(a) Factually accurate or, in the case of estimates and judgements, fairly and properly based after appropriate 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.

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; 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 on the happening 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 needs to have access to a licensee's documents and personnel. Such requests will be made during reasonable business hours and with proper notice. There may be instances where the CBB may seek access to the licensee's premises without prior notice. While such visits are not common, the prospect of unannounced visits is intended to encourage licensees to comply at all times with the requirements and standards imposed by the CBB as per legislation and Volume 6 of the CBB Rulebook.

CRA-11.4.3 The CBB considers 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 may be reasonably requested;

(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) Permit 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 may be reasonably requested; and

CRA-11.4 Methods of Information Gathering (continued)

(f) Answer truthfully, fully and promptly all questions which representatives or appointees of the CBB reasonably put to it.

CRA-11.4.4 The CBB considers that a licensee should take reasonable steps to 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 In gathering information to fulfil its supervisory duties, the CBB acts in a professional manner and with due regard to maintaining confidential information obtained during the course of its information gathering activities.

CRA-11.5 The Role of the Appointed Expert

Introduction

CRA-11.5.1 **The content of this Chapter is applicable to all licensees and appointed experts.**

CRA-11.5.2 The purpose of the contents of this Chapter is to set out the roles and responsibilities of appointed experts when appointed pursuant to Article 114 or 121 of the CBB Law. These Articles empower the CBB to assign some of its officials or others to inspect or conduct investigations of licensees.

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 efforts. In addition, the CBB may commission reports on matters relating to the business of licensees in order to help it assess their compliance with CBB requirements. Inspections may be carried out either by the CBB's own officials, by duly qualified appointed experts appointed for the purpose by the CBB, or a combination of the two.

CRA-11.5.4 The CBB will not, as a matter of general policy, publicise the appointment of an appointed expert, although it reserves the right to do so where this would help achieve its supervisory objectives. Both the appointed expert and the CBB are bound to confidentiality provisions restricting the disclosure of confidential information with regards to any such information obtained in the course of the investigation.

CRA-11.5.5 **Unless the CBB otherwise permits, appointed experts should not be the same firm appointed as external auditor of the licensee. In appropriate circumstances, the CBB may approve the appointment of the licensee's external auditor as appointed expert.**

CRA-11.5.6 **Appointed experts will be appointed in writing, through an appointment letter, by the CBB. In each case, the CBB will decide on the range, scope and frequency of work to be carried out by appointed experts.**

CRA-11.5.7 All proposals to appoint appointed experts require approval by ~~an Executive~~ a Director or more senior official of the CBB. 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 investigation.

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 ~~(but is usually shared by the CBB with the firm concerned)~~.**

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. Commissioned 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**~~ ~~**Unless otherwise directed by the CBB or unless the circumstances described in Paragraph CRA-11.5.18 apply, the report must be discussed with the Board of directors and/or senior management in advance of it being sent to the CBB.**~~

CRA-11.5 The Role of the Appointed Expert (continued)

~~CRA-11.5.15~~ ~~Where the report is qualified by exception, the report must clearly set out the risks which the licensee runs by not correcting the weakness, with an indication of the severity of the weakness should it not be corrected. Appointed experts will be expected to report on the type, nature and extent of any weaknesses found during their work, as well as the implications of a failure to address and resolve such weaknesses.~~

~~CRA-11.5.16~~ ~~If the appointed experts conclude, after discussing the matter with the licensee, that they will give a negative opinion (as opposed to one qualified by exception) or that the issue of the report will be delayed, they must immediately inform the CBB in writing giving an explanation in this regard.~~

~~CRA-11.5.17~~ ~~The report must be completed, dated and submitted, together with any comments by directors or management (including any proposed timeframe within which the licensee has committed to resolving any issues highlighted by the report), to the CBB within the timeframe applicable.~~

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 The CBB recognises that appointed experts cannot be expected to be aware of all circumstances which, had they known of them, would have led them to make a communication to the CBB as outlined above. It is only when appointed experts, in carrying out their duties, become aware of such a circumstance that they should make detailed inquiries with the above specific duty in mind.

CRA-11.5 The Role of the Appointed Expert (continued)

~~CRA-11.5.20~~ ~~If appointed experts decide to communicate directly with the CBB in the circumstances set out in Paragraph CRA-11.5.18, they may wish to consider whether the matter should be reported at an appropriate senior level in the licensee at the same time and whether an appropriate senior representative of the licensee should be invited to attend the meeting with the CBB.~~

Permitted Disclosure by the CBB

CRA-11.5.21 **Information which is confidential and has been obtained under, or for the purposes of, this chapter or the CBB Law may only be disclosed by the CBB in the circumstances permitted under the Law. This will allow the CBB to disclose information to appointed experts to fulfil their duties. It should be noted, however, that appointed experts must keep this information confidential and not divulge it to a third party except with the CBB's permission and/or unless required by Bahrain Law.**

Trilateral Meeting

CRA-11.5.22 The CBB may, at its discretion, call for a trilateral meeting(s) to be held between the CBB and representatives of the relevant licensee and the appointed experts. This meeting will provide an opportunity to discuss the appointed experts' examination of, and report on, the licensee.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-12 Conduct of Business Obligations

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 and organisation 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 The conflicts of interest policy established in accordance with Paragraph CRA-12.2.4 of these Rules must, as 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 in accordance these Rules and must take all appropriate measures to address any deficiencies.

CRA-12.2.6 Licensees must establish, implement and maintain an effective conflicts of interest policy set out in writing and which is appropriate to the size and organisation 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 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 themselves, 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;

(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, 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 employees 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 employees 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 must be maintained.**

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 ~~accepted~~ 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 ~~accepted~~ 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 ~~accepted~~ 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) Seek to avoid conflicts of interest;

(h) Not exert undue pressure or undue influence on a client;

(i) Give advice only on those ~~accepted~~ crypto-assets or regulated crypto-asset services in which the licensee is knowledgeable and seek or recommend other specialist advice when necessary;

(j) Treat all information supplied by the client with complete confidentiality; and

(k) Not request clients to sign declarations to the effect that she/he has understood and accepts certain features of the virtual financial asset or that she/he is relying on his/her own skill, judgement and expertise when it is the obligation of the licensee to assess the suitability or the appropriateness of such ~~accepted~~ crypto-asset vis-à-vis the client.

CRA-12.3 Sale Processes and Selling Practices (Continued)

CRA-12.3.2 Subject to Rule CRA-12.3.3, a licensee and its officers, employees and representatives must maintain, and aid in maintaining, the confidentiality of all clients' information that:

(a) Comes to the knowledge of the licensee, or any of its officers, employees or representatives; and

(b) Is in possession of the member, or any of its officers, employees or representatives.

CRA-12.3.3 Rule CRA-12.3.2 shall not apply to:

(a) The disclosure of client information for such purposes, or in such circumstances as the CBB may prescribe;

(b) Any disclosure of client information which is authorised by the CBB to be disclosed or furnished; or

(c) The disclosure of client information pursuant to any requirement imposed under any law or order of court in 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 Licensees must:

(a) Acknowledge receipt to the client of all money received in connection with an ~~accepted~~ crypto-asset and/or regulated crypto-asset service and that any charge or fee imposed must be disclosed separately;

(b) Have printed on the receipt or contract note, the full name, business address, licensing category of the licensee;

(c) Show the full name and address and official means of identification of the client in the receipt, invoice or contract note;

(d) Make reference in the receipt, invoice or contract note to the type of ~~accepted~~ crypto-asset or regulated crypto-asset service in respect of which the money was paid;

(e) Show, on the receipt, invoice or contract note, the name and address of the crypto-asset exchange from which the ~~accepted~~ crypto-asset was purchased or sold; and

(f) Sign and date the receipt, invoice or contract note and give the original to the client.

CRA-12.3 Sale Processes and Selling Practices (Continued)

Assessment of Clients' Suitability and Appropriateness

CRA-12.3.6 Licensees must ensure that natural persons giving advice or information about ~~accepted~~ crypto-assets or regulated crypto-services to clients on behalf of the licensee possess the necessary knowledge and competence to fulfil their obligations under these Rules.

Suitability

CRA-12.3.7 Licensees must understand the ~~accepted~~ crypto-assets it offers or recommends, assess the compatibility of the ~~accepted~~ crypto-assets with the needs of the clients to whom it provides regulated crypto-asset service, and ensure that ~~accepted~~ crypto-assets are offered or recommended only when this is in the interest of the client.

CRA-12.3.8 Licensees must implement policies and procedures to enable them to collect and assess all information necessary to conduct a suitability assessment for each client.

CRA-12.3.9 Licensees must not create any ambiguity or confusion about their responsibilities in the process when assessing the suitability of ~~accepted~~ crypto-assets or regulated crypto-asset services. When undertaking the suitability assessment, the licensee must inform clients or potential clients, clearly and in simple language, that the reason for assessing suitability is to enable the licensee to act in the client's best interest.

CRA-12.3.10 When providing investment advice or portfolio management services to a client, the licensee must first obtain the necessary information regarding the client's:

(a) knowledge and experience in the investment field relative to the specific type of the ~~accepted~~ crypto-assets or regulated crypto-asset services;
(b) financial situation including the client's ability to bear losses; and
(c) investment objectives including risk tolerance;

CRA-12.3 Sale Processes and Selling Practices (Continued)

CRA-12.3.11 **When providing advice or portfolio management services that involve switching investments, either by selling an ~~accepted~~ crypto-assets and buying another, or by exercising a right to make a change in regard to an existing ~~accepted~~ crypto-assets, a licensee must collect the necessary information on the client's existing investments and the recommended new ~~accepted~~ crypto-assets to undertake an analysis of the costs and benefits of the switch, such that the licensee is reasonably able to demonstrate that the benefits of switching are greater than the costs.**

CRA-12.3.12 **Licensees when providing advice or portfolio management services to a client must, before the transaction is made, provide the Client with a suitability statement.**

CRA-12.3.13 **The suitability statement referred to in Paragraph CRA-12.3.12 must, as a minimum:**

(a) specify the client's financial demands and needs;

(b) provide an outline of the advice given; and

(c) explain why the licensee has concluded that the recommended transaction is suitable for the client, including how it meets the client's objectives and personal circumstances with reference to the investment term required, client's knowledge and experience and client's attitude to risk and capacity for loss.

CRA-12.3.14 Where a licensee provides a regulated crypto-asset service that involves periodic suitability assessments and reports, the subsequent reports after the initial service is established may only cover changes in the ~~accepted~~ crypto-assets involved and/or the circumstances of the client and may not need to repeat all the details of the first report.

Appropriateness

CRA-12.3.15 **When providing a service other than investment advice or portfolio management, a licensee must ask the client to provide information regarding his knowledge and experience in the field relevant to the specific type of ~~accepted~~ crypto-asset or regulated crypto-asset service offered or demanded so as to enable the licensee to assess whether the regulated crypto-asset service or ~~accepted~~ crypto-asset envisaged is appropriate for the client.**

CRA-12.3 Sale Processes and Selling Practices (Continued)

CRA-12.3.16 Licensees must determine whether the client has the necessary experience and knowledge in order to understand the risks involved in relation to the ~~accepted~~ crypto-asset or regulated crypto-asset service offered or demanded when assessing whether a regulated crypto-asset service, other than investment advice or portfolio management, is appropriate for a client.

CRA-12.3.17 In case the licensee considers, on the basis of the information received, that the ~~accepted~~ crypto-asset or regulated crypto-asset service is not appropriate to the client, the licensee must warn the client. This warning may be provided in a standardised format.

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 financial instrument 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 retail 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 for 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. ~~a period of 10 years from the date the agreement comes into force, for CBB's supervision purposes~~.**

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 these Rules (Section CRA-12.5).

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 must be 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 must be 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, 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 Chapter (CRA-13) contains Rules relating to the prohibition of market abuse and market manipulation in accepted crypto-assets and is issued under the powers available to the CBB under Article 38 of the CBB Law, read with the abovementioned provisions of the CBB Law.~~

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 full set of requirements of Module Prohibition of Market Abuse and Manipulation (Module MAM). Licensees and issuers of digital tokens must adhere to the requirements, as laid down in Module MAM, pertaining 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 freezing accounts).

CRA-13.1.1D **A licensees must notify the CBB as soon as practicable 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

Market Surveillance System

CRA-13.1.1E In addition to internal market surveillance policies and controls referred to in Paragraph CRA-13.1.1B 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 for the CBB to perform its own surveillance functions when required.

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** The provisions under this Section applies to all market participants and relevant persons, in Bahrain or outside of Bahrain, including but not limited to crypto-asset offeror (token offeror) or any person acting on their behalf, licensees providing regulated crypto-asset services or any person acting on their behalf and any other person who engages or encourages others to engage in any transactions, in Bahrain or outside Bahrain, in accepted crypto-assets on a licensed crypto-asset exchange.~~

~~Accepted Market Practices~~

~~**CRA-13.1.3** Accepted market practices are those practices that are reasonably expected on one or more financial markets and are accepted by the CBB.~~

~~CRA-13.1 General Requirements (continued)~~

~~CRA-13.1.4 When assessing whether a market practice is acceptable, the CBB will take at least the following criteria into account:~~

~~(a) The level of transparency of the relevant market practice to the whole market;~~

~~(b) The disclosure requirement of the relevant market practice by the market participants;~~

~~(c) The need to safeguard the operation of market forces and the interplay of supply and demand, or safeguard the interest of the investors;~~

~~(d) The degree to which the relevant market practice has an impact on market liquidity and efficiency;~~

~~(e) The degree to which the relevant practice takes into account the trading mechanism of the relevant market and enables market participants to react properly and in a timely manner to the new market situation created by that practice;~~

~~(f) The risk inherent in the relevant practice for the integrity of directly or indirectly, related markets, whether regulated or not, in the relevant accepted crypto-assets within Bahrain;~~

~~(g) The outcome of any inspection or investigation of the relevant market practice by the CBB, by any other authority or market operator with which the CBB cooperates, by any other authority or market undertaking acting on behalf or on the authority of the CBB, or by the courts acting on a referral from the CBB, in particular whether the relevant market practice breached Rules or regulations designed to prevent market abuse, or codes of conduct, be it on the market in question or on directly or indirectly related markets within Bahrain;~~

~~(h) The structural characteristics of the relevant market including whether it is regulated or not, the types of assets traded and the type of market participants, including the extent of non-professional investor participation in the relevant market~~

CRA-13.2 ~~Market Abuse~~ [This Section was deleted in XX 2022]

~~CRA-13.2.1 Market abuse means the manipulation or attempted manipulation of an accepted crypto-asset through the employment of a strategy that may be carried out (whether by one person alone or by two or more persons jointly or in concert) by any available means of trading or other means and:~~

~~(a) Which occurs in relation to accepted crypto-assets traded on a licensed crypto-asset exchange;~~

~~(b) Which satisfies any one or more of the conditions set out in Paragraph CRA-13.2.2; and~~

~~(a) Which is likely to be regarded by a regular user of that market who is aware of the behaviour or conduct as a failure on the part of the person or persons concerned to observe the standard of behaviour or conduct reasonably expected of a person in his or their position in relation to the market;~~

~~CRA-13.2.2 The conditions referred to in Paragraph CRA-13.2.1(b) are that:~~

~~(a) The behaviour or conduct is based on information which is not generally available to those using the market but which, if available to a regular user of the market, would or would be likely to be regarded by him as relevant when deciding the terms on which dealings or transactions in accepted crypto-assets of the kind in question should be effected;~~

~~(b) The behaviour or conduct is likely to give a regular user of the market a false or misleading impression as to the supply of, or demand for, or as to the price or value of, accepted crypto-assets of the kind in question;~~

~~(c) A regular user of the market would, or would be likely to, regard the behaviour or conduct as behaviour or conduct which would, or would be likely to, distort the market in accepted crypto-assets of the kind in question.~~

~~CRA-13.2.3 The types of behaviour or conduct that amount to market abuse include:~~

~~**(a)** Abuse of information:~~

~~(i) Insider dealing;~~

~~(ii) Improper disclosure;~~

~~(iii) Misuse of information.~~

~~**(b)** Market manipulation:~~

~~(i) Manipulating transactions;~~

~~(ii) Manipulating devices;~~

~~(iii) Dissemination;~~

~~(iv) Misleading behaviour and distortion.~~

~~CRA-13.2 Market Abuse (continued)~~

~~CRA-13.2.4 Market manipulation, misleading behaviour or conduct, insider trading and fraudulent or deceptive behaviour or conduct may distort the price discovery system and distort prices and thereby unfairly disadvantage the investors. Any person who is engaged in, or encourages others to engage, in any manner, in any conduct that leads to or may lead to market manipulation, misleading behavior, insider trading and fraudulent or deceptive behavior is guilty of an offence of market manipulation.~~

~~CRA-13.2.5 In application of CRA-13.2.4, the CBB will consider that a person is guilty of market manipulation if the person engages or encourages to engage in any act of commission of omission prohibited under this Section.~~

~~CRA-13.2.6 A person shall not be guilty of market manipulation if he proves that his reasons for engaging in the alleged behaviour or conduct were legitimate and that he had acted in conformity with the accepted market practices in the market concerned.~~

~~Role of Licensees~~

~~CRA-13.2.7 All licensees in general, and licensed crypto-asset exchange in particular, must have in place effective systems, procedures and arrangements to monitor and detect market abuse and where it suspects that there may exist circumstances to indicate that any violation of the provisions under this Section have been committed, is being committed or is likely in the circumstances to be committed, it must immediately report such suspicion to the CBB in the format given in Paragraph CRA-13.2.8.~~

CRA-13.2 Market Abuse (continued)

CRA-13.2.8	**Any information which may be of significance (along with a list of any accompanying documents/evidence)**
	Details of the person making notification *Name of person, name of firm, position held within firm, contact details, etc.*
	Signed …….. (*person making report***)** **Dated …….. (***date of report***)**
	Description of the transaction(s) *Details of the accepted crypto-assets,; the market(s) concerned; the original order's entry date/ time, price and size; the times and sizes of the transaction(s); the type and characteristics of the order, etc.*
	Reasons for Suspicion *Reasons for suspecting that the transaction(s) might constitute insider dealing/ market abuse/ market manipulation*
	Identities of persons carrying out transaction(s) *Names, addresses, telephone number, location, account number, client Identification code used by the firm, etc.*
	Identities of any other persons known to be involved in the transaction(s) *Names, addresses, telephone number, location, relation to person carrying out the transaction, position held, role played, etc.*

CRA-13.2 Market Abuse (continued)

CRA-13.2.9 Where the information specified to be reported is not available at the time of reporting, the report shall include at least the reasons why the reporting persons suspect that the transactions might constitute insider dealing or market manipulation. All remaining information shall be provided to the CMSD as soon as it becomes available.

Persons making suspicious transactions reports therefore, do not need to have all the required information before contacting the CMSD. If the case is one which (the persons subject to the reporting obligation consider) needs to be brought to the attention of the CMSD urgently, then the person(s) concerned shall make the first contact quickly. This can be done by telephone if appropriate, giving the basic details and reasons for suspicion, followed by written confirmation. The other information can be supplied subsequently.

CRA-13.2.10 A person must not inform, disseminate, or certify any statement or information which is false or may cause material misunderstanding about financial condition, results of business operation, any other information related to the price of an accepted crypto-asset in such manner that is likely to have an impact on the accepted crypto-asset price or the decision to invest in accepted crypto-asset.

CRA-13.2.11 A person must not analyse or forecast the financial condition, the results of business operation, any other information related to an accepted crypto-asset, the characteristics or particulars of accepted crypto-asset or the price of accepted crypto-asset by using information known to be false or incomplete which may cause material misunderstanding in the making of such analysis or forecast, or neglect to consider the accuracy of such information, or by distorting the information used in the making of the analysis or the forecast, and disclose or give an opinion about such analysis or forecast to the public in such manner that is likely to have an impact on the accepted crypto-asset price or decision to invest in accepted crypto-asset.

CRA-13.2.12 A person who is aware or in possession of the inside information related to an accepted crypto-asset must not purchase or sell accepted crypto-asset or enter into a derivatives contract related to accepted crypto-asset, either for his or her own benefit or for the benefit of any other persons, except such action is undertaken in compliance with the Law, Rules and regulations.

CRA-13.3 ~~Prohibited Conduct with respect to Possession of Inside Information~~ [This Section was deleted in XX 2022]

~~CRA-13.3.1 A person who is aware or in possession of the inside information related to an accepted crypto-asset must not use such information to:~~

~~(a) Deal in any accepted crypto-asset to which that information relates;~~

~~(b) Encourage any person to deal in any accepted crypto-asset to which that information relates;~~

~~(c) Disclose inside information to any other person, either directly or indirectly and by any means, where such person knows or ought to know that the receiver of such information may exploit such information for purchasing or selling the accepted crypto- assets, either for the his or her own benefit or for the benefit of any other persons, except where such action is in the manner which does not take advantage of any other persons or in the proper performance of the functions of his employment, office or profession;~~

~~(d) Violate the Rules governing the publishing of market information.~~

~~CRA-13.3.2 For the purposes of this Module, "Inside information" means information that:~~

~~(a) Is precise in nature relating directly or indirectly to one or more of the accepted crypto-asset;~~

~~(b) Has not been made public;~~

~~(c) If made public, is likely to have a significant impact on the price of those accepted crypto-asset;~~

~~CRA-13.3.3 For the purpose of this Module, "Insider" means any person who has obtained inside information;~~

~~(a) By virtue of his employment or profession;~~

~~(b) Being an officer or crypto-asset holder of the crypto-asset offer; or~~

~~(c) Through illegal means.~~

~~A person is an insider if he is already aware that such information is classified as inside information even though none of the above applies to him.~~

~~CRA-13.3 Prohibited Conduct with respect to Possession of Inside Information (continued)~~

~~All persons who have access or come into possession of material inside information before its public release are considered insiders. Such persons include controlling shareholders, "directors and senior management", officers and employees, and frequently should also include any officials of the CBB and the crypto-asset exchange who have access to such information, outside attorneys, accountants, auditors, public relations advisers, advertising agencies, consultants and other independent contractors.~~

~~The husbands, wives, immediate families and those under the control of insiders may also be regarded as insiders. Further, for purposes of this Module, insiders include "tippees" who come into possession of material inside information.~~

~~CRA-13.3.4 The insider must not (whether as principal or agent):~~

~~(a) Subscribe for, purchase or sell, or enter into an agreement to subscribe for, purchase or sell any such accepted crypto-assets; or~~

~~(b) Procure another person to subscribe for, purchase or sell, or to enter into an agreement to subscribe for, purchase or sell, any such accepted crypto-assets.~~

CRA-13.4 ~~Prohibited Market Conduct~~ [This Section was deleted in XX 2022]

~~CRA-13.4.1 For the purposes of this Module, a person is guilty of market abuse manipulation if he engages or encourages to engage in any conduct that may give a false or misleading impression as to the supply of or demand for, or the price or value of any accepted crypto-asset or that may give an unrealistic picture of the market regarding the volume and/or prices of any accepted crypto-asset.~~

~~CRA-13.4.2 In application of Paragraph CRA-13.4.1, the CBB will consider that a person is guilty of market manipulation if he engages or encourages to engage in any act of commission or omission of the prohibited market behaviour or conduct listed in Rule CRA-13.4.3.~~

~~CRA-13.4.3 No person shall directly or indirectly:~~

~~(a) Engage or encourage others to engage in any behaviour or conduct that may give a false or misleading impression as to the supply of or demand for, or the price or value of any accepted crypto-assets.~~

~~(b) Engage or encourage others to engage in any behaviour or conduct that may give an unrealistic picture of the market regarding the volume and/or prices of any accepted crypto-assets.~~

~~(c) Create or do anything that is intended or likely to create a false or misleading appearance:~~

~~(i) Of active trading in any accepted crypto-assets on a market;~~

~~(ii) With respect to the market for, or the price of, such accepted crypto-assets; or~~

~~(iii) By engaging or encouraging others to engage in any act of conducting or attempting to conduct a manoeuver with the intention to impede normal functioning of a market.~~

~~(d) Maintain, inflate, depress, stabilize, or cause fluctuations in the market price of any securities, or the trading volume of any accepted crypto-assets by means of a purchase or sale of any accepted crypto-assets that do not involve a change in the beneficial ownership of those accepted crypto-assets, or by any fictitious transaction or device.~~

~~(e) Engage or encourage others to engage in any fraudulent or misleading or manipulative practice, such as to:~~

~~(i) Employ any device, scheme or artifice to defraud;~~

~~(ii) Buy, sell, intermediate or otherwise deal in accepted crypto-assets in a fraudulent manner~~

CRA-13.4 Prohibited Market Conduct (continued)

(iii) Obtain money or property by means of any untrue statement of a material fact or any omission to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading;

(iv) Engage in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser; or

(v) Induce, fraudulently, other persons to deal in accepted crypto-assets.

(f) Use or employ, purchase or sale of any accepted crypto-asset listed in a licensed crypto-asset exchange, any manipulative or deceptive device or contrivance in contravention of the provisions of the CBB Law or the Rules and regulations made thereunder, including the Rules and regulations of licensed crypto-asset exchanges.

(g) Manipulate or publish or cause to publish or report or cause to report by a person dealing in accepted crypto-assets any information which is not true or which he does not believe to be true prior to or in the course of dealing in accepted crypto-assets.

(h) Indulge in price manipulation or any act or omission amounting to manipulation of the price or volume of an accepted crypto-asset.

(i) Make a statement, promise, forecast or any other action, or disseminate information that is false or misleading and has or is likely to have an impact on the price or volume of accepted crypto-assets.

(j) Employ manipulative or deceptive devices or practices.

(k) Fail, intentionally or recklessly, to notify the CBB of such information as is required to be disclosed as per the CBB Law, Rules and regulations, this Module and AML/CFT of CBB's Rulebook Volume 6.

(l) Indulge in manipulative or fraudulent or unfair trade practices in accepted crypto-assets.

(m) Provide clients with such information relating to an accepted crypto-asset that cannot be verified by the clients before their dealing in such accepted crypto-asset.

(n) Encourage clients to deal in accepted crypto-assets solely with the object of enhancing his brokerage or commission.

(o) Indulge in buying or selling in accepted crypto-assets in advance of a substantial client order.

(p) Plant false or misleading news or rumours, or deceitful information which may induce sale or purchase of accepted crypto-assets.

~~CRA-13.4 Prohibited Market Conduct (continued)~~

~~CRA-13.4.4 In any proceedings against a person for a contravention of Rule CRA-13.4.3 (c) and (d) because of an act referred to in Rule CRA-13.4.3, it is a defence if the defendant establishes that the purpose or purposes for which he did the act was not, or did not include, the purpose of creating a false or misleading appearance of active trading in accepted crypto-assets on a market.~~

~~CRA-13.4.5 For the purposes of Rule CRA-13.4.3 (c) and (d) and Rule CRA-13.4.3, a purchase or sale of accepted crypto-assets does not involve a change in the beneficial ownership if a person who had an interest in the accepted crypto-assets before the purchase or sale, or a person associated with the first-mentioned person in relation to those accepted crypto-assets, has an interest in the accepted crypto-assets after the purchase or sale.~~

CRA-13.5 ~~False Trading and Market Rigging Transactions~~ [This Section was deleted in XX 2022]

~~CRA-13.5.1 Without prejudice to the provisions of the Rule CRA-13.4.3, a person who:~~

~~(a) Effects, takes part in, is concerned in or carries out directly or indirectly, any transaction of purchase or sale of any accepted crypto-assets, being a transaction that does not involve any change in the beneficial ownership of the accepted crypto-assets;~~

~~(b) Makes or causes to be made an offer to sell any accepted crypto-assets at a specified price where he has made or caused to be made or proposes to make or to cause to be made, or knows that a person associated with him has made or caused to be made or proposes to make or to cause to be made, an offer to purchase the same number, or substantially the same number of accepted crypto-assets at a price that is substantially the same as the first mentioned price; or~~

~~(c) Makes or causes to be made an offer to purchase any accepted crypto-assets at a specified price where he has made or caused to be made or proposes to make or to cause to be made, or knows that a person associated with him has made or caused to be made or proposes to make or to cause to be made, an offer to sell the same number, or substantially the same number, of securities at a price that is substantially the same as the first-mentioned price, is deemed to have created a false or misleading appearance of active trading in accepted crypto-assets on a market.~~

~~CRA-13.5.2 For the purposes of this Module, the term "Beneficial Owner" refers to any person who, even if not the recorded owner of the accepted crypto-assets, has or shares the underlying benefits of ownership. These benefits include the power to direct the disposition of the accepted crypto-assets, or to receive the economic benefit of ownership of the accepted crypto-assets. A person is also considered to be the "beneficial owner" of accepted crypto-assets if that person has the right to acquire such accepted crypto-assets within a certain period of time, either by option or other agreement. Beneficial owners include persons who hold their accepted crypto-assets through one or more trustees, brokers, agents, legal representatives or other intermediaries.~~

~~CRA-13.5.3 In any proceedings against a person for a contravention of Rule CRA-13.5.1 in relation to a purchase or sale of securities that did not involve a change in the beneficial ownership of those accepted crypto-assets, it is a defence if the defendant establishes that the purpose or purposes for which he purchased or sold the accepted crypto-assets was not, or did not include, the purpose of creating a false or misleading appearance with respect to the market for, or the price of, accepted crypto-assets.~~

~~CRA-13.5 False Trading and Market Rigging Transactions (continued)~~

~~CRA-13.5.4 The reference in Rule CRA-13.5.1 to a transaction of purchase or sale of accepted crypto-assets includes: (a) A reference to the making of an offer to purchase or sell accepted crypto-assets; and (b) A reference to the making of an invitation, however expressed, that expressly or impliedly invites a person to offer to purchase or sell accepted crypto-assets.~~

CRA-13.6 ~~Fraudulent Dealings~~ [This Section was deleted in XX 2022]

~~*Fraudulently Inducing Persons to Deal in Accepted Crypto-Assets*~~

~~CRA-13.6.1 Without prejudice to the provisions of Rule CRA-13.4.3 (e), a person must not induce or attempt to induce another person to deal in accepted crypto-assets:~~

~~(a) By making or publishing, by any means, any statement, promise or forecast that he knows or ought reasonably to have known to be misleading, false or deceptive;~~

~~(b) By any dishonest concealment of material facts;~~

~~(c) By the reckless making or publishing of any statement, promise or forecast that is misleading, false or deceptive; or~~

~~(d) By recording or storing in, or by means of, any mechanical, electronic or other device information that he knows to be false or misleading in a material particular.~~

~~CRA-13.6.2 In any proceeding against a person for a contravention of Rule CRA-13.6.1 constituted by recording or storing information as mentioned in Rule CRA-13.6.1 (d), it is a defence if it is established that, at the time when the defendant so recorded or stored the information, he had no reasonable grounds for expecting that the information would be available to another person.~~

~~*Employment of Manipulative and Deceptive Devices or Practices*~~

~~CRA-13.6.3 Without prejudice to the provisions of Rule CRA-13.4.3 (c), a person must not, directly or indirectly, in connection with the subscription, purchase or sale of any accepted crypto-assets:~~

~~(a) Employ any device, practice, scheme or artifice to defraud;~~

~~(b) Engage in any act or course of business which operates as a fraud or deception, or is likely to operate as a fraud or deception, upon any person;~~

~~(c) Make any statement he knows to be false in a material particular; or~~

~~(d) Omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading~~

CRA-13.7 ~~Dissemination of False or Misleading Statements~~ [This Section was deleted in XX 2022]

~~CRA-13.7.1 Without prejudice to the provisions of section CRA-13.4, no person shall circulate or disseminate, or authorise or be concerned in the circulation or dissemination of, any statement or information which is false or may cause material misunderstanding about financial condition, result of business operation, any other information related to the characteristic or particulars of accepted crypto-assets, in such a manner that is likely to have an impact on the accepted crypto-asset price or the decision to invest in accepted crypto-assets.~~

~~CRA-13.7.2 Without prejudice to the provisions of Rule CRA-13.4.3 (e) and (f), a person must not make a statement, or disseminate information, that is false or misleading in a manner that particular and is likely:~~

~~(a) To induce the sale or purchase of accepted crypto-assets by other persons; or~~

~~(b) To have the effect of raising, lowering, maintaining or fixing the market price of accepted crypto-assets, if, when he makes the statement or disseminates the information;~~

~~(c) He does not care whether the statement or information is true or false; or~~

~~(d) He knows or ought reasonably to have known that the statement or information is false or misleading in a material particular.~~

CRA-13.8 ~~Price Manipulation~~ [This Section was deleted in XX 2022]

~~CRA-13.8.1 Without prejudice to the provisions of Rule CRA-13.4, a person must not effect, take part in, be concerned in or carry out, directly or indirectly, two or more transactions in accepted crypto-assets, being transactions that have, or are likely to have, the effect of raising, lowering, maintaining or fixing the price of accepted crypto-assets on a market, with intent to induce other persons to purchase or sell accepted crypto-assets.~~

CRA-13.9 ~~Methods to Market Abuse and Manipulation~~ [This Section was deleted in XX 2022]

~~CRA-13.9.1 A person who engages or encourages others to engage in market manipulation by his acts of commission or omission will be liable for financial penalties and/or other enforcement actions, irrespective of the methods used for market manipulation or the objective of such manipulative market behaviour or conduct. Methods of market abuse and market manipulation may include but not be limited to the methods as mentioned below:~~

~~1) Abuse of Information:~~

~~(a) Insider Dealing~~

~~i. Front running~~

~~ii. Tail gating~~

~~iii. Spreading false information to purchase at bargain prices~~

~~(b) Misuse of Information~~

~~i. Pump and Dump~~

~~ii. Trash and Crash~~

~~iii. Influencing market price without controlling the available supply or demand~~

~~iv. Boiler room sales~~

~~v. Cyber smear~~

~~vi. Scalping~~

~~vii. False market~~

~~viii. Short and Distort (Bear Raid)~~

~~ix. Long and Distort~~

~~2) Market Manipulation:~~

~~(a) Manipulating Transactions~~

~~i. Painting the tape~~

~~ii. Wash sales~~

~~iii. Improper matched orders~~

~~iv. Marking the close~~

~~v. Cornering the market~~

~~vi. Abusive squeeze~~

~~vii. Capping and Pegging~~

~~viii. Pooling and churning~~

~~ix. Interpositioning~~

~~x. Ghosting~~

~~xi. Bucketing~~

~~(b) Manipulating Devices:~~

~~i. Advancing the bid~~

~~ii. Placing order without intention to execute~~

~~iii. Excessive bid-ask spread~~

~~CRA-13.9 Methods to Market Abuse and Manipulation (continued)~~

~~(c) Misleading Behaviour and Distortion~~

~~i. Short and extort~~

~~ii. Spoofing~~

~~iii. Overtrading~~

~~CRA-13.9.2 The CBB would investigate into the intentions behind the market behaviour or conduct and the objectives of the market behaviour or conduct of the various parties while dealing with suspected market behaviour or conduct cases.~~

CRA-14.1 ~~General Procedures~~ [This Section was deleted in XX 2022]

~~The CBB's Approach to Enforcement~~

~~CRA-14.1.1 The CBB favours an open, pragmatic and collaborative relationship with authorised persons, within the boundaries set by the CBB Law and Rulebook. Whilst the CBB wishes to avoid a legalistic and confrontational style of supervision, it believes that effective supervision requires effective and timely enforcement of its requirements. Should licensees fail to cooperate, then the CBB will use the means described in this section to achieve compliance.~~

~~CRA-14.1.2 In the CBB's view, it is generally neither practical nor effective to prescribe in detail the exact regulatory response for each and every potential contravention. There are a large number of potential contraventions. Moreover, individual circumstances are unlikely to be identical in all cases, and may warrant different responses.~~

~~CRA-14.1.3 In deciding any given supervisory response, the CBB will nonetheless consistently assess the individual circumstance of each contravention against the principles described in this Module. The CBB's overall approach is to take into account:~~

- ~~(a) The seriousness of the contravention concerned (including the risks posed to customers and other market participants);~~
- ~~(b) The compliance track record of the licensee concerned (including the extent to which the contravention reflects systemic weaknesses or reckless behaviour); and~~
- ~~(c) Which measures are most likely to achieve the desired result of remedying the contravention.~~

~~CRA-14.1.4 Such an approach reduces the risk of inappropriate enforcement actions, by allowing regulatory measures to be tailored to individual circumstances. By taking into account a licensee's compliance record and attitude, it also creates positive incentives and encourages an open and collaborative approach. By assessing individual cases against the same broad principles, the CBB also aims to achieve an overall consistency in its regulatory actions.~~

~~CRA-14.1.5 Underlying the CBB's approach outlined in Paragraph CRA-14.1.3 is the fundamental principle of proportionality. The enforcement measures contained in this section are of varying severity, and will be used accordingly in keeping with the CBB's assessment of the contravention. Thus, the CBB will reserve its most serious enforcement measures – such as cancellation of license or withdrawal of "fit and proper" status – for the most serious contraventions.~~

~~CRA-14.1.6 In keeping with the proportionality principle, and to the extent consistent with the CBB's enforcement approach in Paragraph CRA-14.1.3, the CBB will usually opt for the least severe of appropriate enforcement measures. In most cases, the CBB expects to use a Formal Warning before resorting to more severe measures; the need for further measures will then usually be dependent on the response of the authorised person concerned.~~

CRA-14.1 General Procedures (continued)

CRA-14.1.7 Where a significant element of judgement is required to assess compliance with a requirement, the CBB will usually discuss the matter with the licensee concerned, before using one of this section's enforcement mechanisms. This is likely to be the case, for example, with respect to requirements for adequate systems and controls. Conversely, where there are clear-cut contraventions of CBB requirements, then the CBB will usually move immediately to one or more of the enforcement mechanisms outlined in this section. This is more likely to occur in cases where quantitative requirements - such as those relating to capital and/or market abuse – are concerned. In most such cases, though, the CBB also expects to continue an active dialogue with the authorised person concerned, aimed at remedying the contravention.

CRA-14.1.8 Except in the limited circumstances outlined below, the CBB will usually only apply an enforcement measure after the licensee or person concerned has been given a suitable opportunity to make representations. In the case of measures described in section CRA-14.7 to CRA-14.10, certain procedures are set out in the Central Bank of Bahrain and Financial Institutions Law (Decree No. 64 of 2006).

Prohibition on Insurance

CRA-14.1.9 To help the CBB achieve the purpose of this Module, licensees may not enter into or make a claim under a contract of insurance that is intended to, or has the effect of, indemnifying them from the fines provided for in this Module.

Publicity

CRA-14.1.10 The CBB will not as a matter of general policy publicise individual cases when it uses the measures set out in Section CRA-14.2 to CRA-14.7. However, in such cases the CBB may inform the licensee's external auditor and – in the case of licensees with overseas operations – relevant overseas regulators.

CRA-14.1.11 In exceptional circumstances, as allowed by Article 132 of the CBB Law, the CBB may decide to publicise individual cases when the measures set out in section CRA-14.6 are used, where there is a strong case that doing so would help achieve the CBB's supervisory objectives. In such instances, the CBB will usually allow the licensee or individual concerned the opportunity to make representations to the CBB before a public statement is issued.

CRA-14.1.12 With respect to the financial penalties provided for in section CRA-14.6, licensees are required to disclose in their annual report the amount of any such penalties paid to the CBB, together with a factual description of the reason(s) given by the CBB for the penalty.

CRA-14.1 General Procedures (continued)

CRA-14.1.13 Without prejudice to the above policy, the CBB may from time to time publish aggregate information on its use of measures set out in section 14.2 to CRA-14.7, without identifying the licensees or individuals concerned, unless their identities have previously been disclosed as provided for in Paragraphs CRA-14.1.11 or CRA-14.1.12.

CRA-14.1.14 By their nature, the penalties in section CRA -14.8 to CRA-14.10 inclusive are public acts, once applied. The CBB will in these instances generally issue a public statement explaining the circumstances of the case.

CRA-14.2 Formal Warnings [This Section was deleted in XX 2022]

CBB Policy

CRA-14.2.1 Formal warnings are clearly identified as such and represent the CBB's first level formal enforcement measure. They are intended to clearly set out the CBB's concerns to a licensee or an individual regarding an issue, and should be viewed by the recipient with the appropriate degree of seriousness.

CRA-14.2.2 As indicated in Section CRA-14.1, the CBB will usually discuss concerns prior to resorting to a formal enforcement measure, especially where a significant element of judgment is required in assessing compliance with a regulatory requirement.

CRA-14.2.3 Where such discussions fail to resolve matters to the CBB's satisfaction, then it may issue a formal warning. Failure to respond adequately to a formal warning will lead the CBB to consider more severe enforcement measures. However, more severe measures may not require the prior issuance of a formal warning – depending on its assessment of the circumstances, the CBB may decide to have immediate recourse to other measures. Similarly, there may be circumstances where the CBB issues a formal warning without prior discussion with the licensee or person concerned: this would usually be the case where a clear-cut compliance failing has occurred.

CRA-14.2.4 When considering whether to issue a formal warning, the criteria taken into consideration by the CBB therefore include the following:

(a) The seriousness of the actual or potential contravention, in relation to the requirement(s) concerned and the risks posed to the licensee's customers, market participants and other stakeholders;

(b) In the case of an actual contravention, its duration and/or frequency of the contravention; the extent to which it reflects more widespread weaknesses in controls and/or management; and the extent to which it was attributable to deliberate or reckless behaviour; and

(c) The extent to which the CBB's supervisory objectives would be better served by issuance of a formal warning as opposed to another type of regulatory action.

Procedure for Issuing Formal Warnings

CRA-14.2.5 Proposals to issue formal warnings are carefully considered against the criteria listed in Section CRA-14.2. They require the approval of a Director or more senior CBB official, and include the statement "This is a formal warning as defined in section CRA-14.2 of the CBB Rulebook".

CRA-14.2.6 Depending on the issue in question, recipients of a formal warning may be required to respond to the contents of the warning. In any case, recipients have the right to object to or challenge a formal warning as specified under Articles 125(c) and 126 of the CBB Law.

CRA-14.3 Directions [This Section was deleted in XX 2022]

CBB Policy

CRA-14.3.1 The CBB may issue Directions to licensees or individuals under supervisory powers granted to it by the CBB Law. These powers are broad in nature, and effectively allow the CBB to issue whatever Directions it reasonably believes are required to achieve its statutory objectives.

CRA-14.3.2 The types of Directions that the CBB may issue in practice vary and will depend on the individual circumstances of a case. Generally, however, Directions require a licensee or individual to undertake specific actions in order to address or mitigate certain perceived risks. They may also include restrictions on a licensee's activities until those risks have been addressed – for instance, a ban on the acceptance of new customers.

CRA-14.3.3 The CBB is conscious of the powerful nature of a Direction and, in the case of a licensee, the fact that it subordinates the role of its Board and management on a specific issue. The CBB will carefully consider the need for a Direction, and whether alternative measures may not achieve the same end. Where feasible, the CBB will try to achieve the desired outcome through persuasion, rather than recourse to a Direction.

CRA-14.3.4 In considering whether to issue a Direction, the criteria taken into consideration by the CBB include the following:

(a) The seriousness of the actual or potential contravention, in relation to the requirement(s) concerned and the risks posed to the licensee's customers, market participants and other stakeholders;

(b) In the case of an actual contravention, its duration and/or frequency of the contravention; the extent to which it reflects more widespread weaknesses in controls and/or management; and the extent to which it was attributable to deliberate or reckless behaviour; and

(c) The extent to which the CBB's supervisory objectives would be better served by issuance of a Direction as opposed to another type of regulatory action.

Procedure for Issuing Directions

CRA-14.3.5 Proposals to issue Directions are carefully considered against the criteria listed in Section CRA-14.3. They require the approval of an Executive or more senior official of the CBB, and include the statement "This is a formal Direction as defined in section CRA-14.3 of the CBB Rulebook".

CRA-14.3.6 The subject of the Direction will normally be given 30 days from the Direction's date of issuance in which to make objections to the CBB concerning the actions required. This must be done in writing, and addressed to the issuer of the original notification. Should an objection be made, the CBB will make a final determination, within 30 days of the date of the objection, as specified in Articles 125(c) and 126 of the CBB Law.

CRA-14.3 ~~Directions (continued)~~

~~CRA-14.3.7 In extreme circumstances, where the CBB believes that immediate action is required to prevent real damage to Bahrain's financial markets, its users or to customers of the licensee concerned, it may cancel or amend a license, as specified in Article 48(g) of the CBB Law, or place a licensee under administration according to Article 130(2) of the CBB Law, or suspend a license according to Article 131 of the pre-mentioned Law. These measures may be used in conjunction with directions.~~

CRA-14.4 ~~Formal Request for Information~~ [This Section was deleted in XX 2022]

~~***Procedure for request of Information***~~

~~CRA-14.4.1 As part of its on-going supervision, under Articles 111, 113, 114, and 123 of the CBB Law, the CBB may specifically request information or temporary reporting from a licensee or individual. Recipients of such requests are bound to respond to such requests under the terms of their license.~~

~~CRA-14.4.2 Henceforward, to clearly identify such requests, they will always be made in writing, under signature of a Director or more senior official of the CBB; will include the statement "This is a formal request for information as defined in section CRA-14.4 of the CBB Rulebook"; and will state the deadline by which the information is to be communicated to the CBB.~~

~~CRA-14.4.3 Failure to respond to such formal requests within the deadline set will be viewed as a significant breach of regulatory requirements and will incur a formal warning or other enforcement measure, specified under Articles 163 and 170 of the CBB Law, as decided by the CBB depending on the circumstances of the case.~~

~~CRA-14.4.4 The deadline set in the request will vary depending on individual circumstances, but will in all cases be reasonable. A recipient may submit a case for an extension to the deadline, providing the request is made before the original deadline has passed. The CBB will respond before the original deadline has passed; if it fails to do so, then the requested extension will apply. Whilst waiting for a reply, the recipient must assume that the original deadline will apply.~~

~~CRA-14.4.5 The above procedures do not prevent individual CBB supervisors making oral requests for information as part of their day-to-day interaction with licensees. The CBB expects licensees to maintain their cooperative response to such requests; however, in the interests of clarity, the CBB will not view failures to respond to oral requests as a breach of regulatory requirements.~~

CRA-14.5 Adverse "Fit and Proper" Findings [This Section was deleted in XX 2022]

Requirements for Individuals

CRA-14.5.1 Article 65 of the CBB Law, allows the CBB to determine the level of qualifications, experience, and training of a licensee's board members, officers or employees.

CRA-14.5.2 In addition, section CRA-1.7 specifies that all persons wishing to hold or holding the position of Director, Chief Executive/General Manager or Manager in a licensee must be assessed by the CBB as "fit and proper" to hold such a position. The section specifies various factors that the CBB takes into account when reaching such a decision.

CRA-14.5.3 Any Director, manager or official responsible for the direction or management of a licensee, is to be considered removed from office should he be convicted by a court for a crime affecting his honesty; is declared bankrupt by a court; or if a court Rules that his legal capacity is totally or partially impaired.

CBB Policy

CRA-14.5.4 The CBB is conscious of the impact that assessing someone as not "fit and proper" may have on an individual. Such assessments are carefully reviewed in the light of all relevant facts. The criteria used in reaching a decision include the following:

(a) The extent to which the factors set out in section CRA-1.7 and MIR-3.1.3 of Module MIR have not been met;

(b) The extent to which the person has deliberately or recklessly breached requirements of the CBB Law and/or this Module;

(c) The person's past compliance record and conduct following any such contravention;

(d) The length of time since factors indicating a lack of fitness or propriety occurred; and

(e) The risk the person poses to licensees and their customers.

CRA-14.5.6 In assessing evidence, the CBB applies a lower threshold than is applied in a criminal court of law, reflecting generally, the administrative nature of the sanction. The CBB may also take into account the cumulative effect of factors which, when considered individually, may not in themselves be sufficient to justify an adverse "fit and proper" finding.

CRA-14.5.7 The CBB may also take into account the particular function being undertaken in the licensee by the individual concerned, and the size and nature of the licensee itself, particularly when assessing the suitability of a person's experience or qualifications. Thus, the fact that a person was deemed "fit and proper" for a particular position in a particular firm does not necessarily mean he would be suitable in a different position or in a different firm.

CRA-14.5 Adverse "Fit and Proper" Findings (continued)

CRA-14.5.8 The CBB may carry out re-assessment tests in case of individuals deemed to be responsible for serious or repeated violations. See Appendix 2

Procedure for Issuing an Adverse Finding

CRA-14.5.8 All proposals for issuing an adverse "fit and proper" finding are subject to a thorough review by the CBB of all relevant facts, assessed against the criteria outlined in section CRA-14.5.4 to CRA-14.5.7. In some instances, it may be appropriate for the CBB to request the licensee or person concerned to provide further information, in order to help reach a decision.

CRA-14.5.9 All adverse findings have to be approved by a Director or more senior official Executive Director of the CBB. A notice of intent is issued to the person concerned, and copied to the Board/senior management of the licensee as appropriate, setting out the circumstances and the basis for the CBB's proposed adverse finding. The person has 30 calendar days from the date of the notice in which to make written representations, addressed to the Executive Director concerned, failing which a final notice is issued by the CBB.

CRA-14.5.10 If representations are made, then the CBB has 30 calendar days from the date of the representation in which to consider any mitigating evidence submitted and make a final determination.

CRA-14.6 Financial Penalties [This Section was deleted in XX 2022]

CBB Policy

CRA-14.6.1 Under Chapter 2 "Procedures to be taken before penalties or administrative proceedings are applied" and Chapter 3 "Penalties and administrative proceedings" of Part 9 of the CBB Law, the CBB may impose financial penalties on licensees or persons referred to in Paragraph (b) of Article (68 bis 1) of the CBB Law and its amendments (in particular Article 129). The CBB shall use judgement and will take into account relevant facts in determining the need to impose financial penalties. Financial penalties are thus normally preceded by the issuance of a written formal notice and/or Direction.

CRA-14.6.2 The level of financial penalty applied is determined by the nature of the contravention and the amount of additional supervisory attention and resources taken up by a licensee's or persons' referred to in Paragraph (b) of Article (68 bis 1) of the CBB Law behaviour and by limits set in the CBB Law. The CBB will apply the methodology set out in Appendix 2 to determine the size of the penalty. The CBB intends that the impact of a penalty should derive more from its signaling effect than from the actual amount of money involved.

CRA-14.6.3 In accordance with Article 129 of the amendment to the CBB Law, the maximum financial penalty levied for failing to comply with CBB Law, Regulations, Directives and other requirements is BD 100,000 per violation. The CBB may opt to limit the amount of the financial penalty and use other enforcement measures as outlined in this Chapter, such as imposing restrictions on a licensee limiting the scope of operations.

CRA-14.6.4 As indicated in Paragraph CRA-14.1.12, the CBB requires disclosure by licensees in their annual report of any financial penalties served on them, together with a factual description of the reasons given by the CBB for applying the penalty. In addition, the CBB may publicise the issuance of a financial penalty notice, where there is a strong case that doing so would help achieve the CBB's supervisory objectives, as mentioned in Article 132 of the pre-mentioned Law.

CRA-14.6.5 Examples of the types of compliance failings that may lead to the serving of a financial penalty notice are outlined in Part 11 of the CBB Law and may include (but are not limited to):

(a) Failures to address persistent delays and/or significant inaccuracies in regulatory reporting to the CBB;

(b) Repeated failures to respond to formal requests for information from the CBB, within the deadlines set;

(c) The submission of information to the CBB known to be false or misleading; and

(d) Major failures in maintaining adequate systems and controls in accordance with the CBB's requirements, subjecting depositors and other customers to significant risk of financial loss.

CRA-14.6 Financial Penalties (continued)

CRA-14.6.6 In assessing whether to serve a financial written penalty notice, the CBB takes into account the following criteria:

(a) The seriousness of the contravention, in relation to the requirement(s) concerned;

(b) The duration and/or frequency of the contravention, and the extent to which it reflects more widespread weaknesses in controls and/or management; the extent to which the contravention was deliberate or reckless;

(c) The licensee's past compliance record and conduct following the contravention; and

(d) The scope of any other action taken by the CBB or other regulators against the licensee, in response to the compliance failures in question.

Additional criteria are set out in Appendix 2.

CRA-14.6.7 The imposition of a financial penalty does not preclude the CBB from also using other enforcement measures to remedy the same violation (for instance, a Direction).

CRA-14.6.8 A written notice of a financial penalty must be issued before imposing any financial penalty. The written notice must contain the following information:

(a) The violations committed by the licensee with respect to CBB Law; or the prudential Rulebook; or any Directions, warnings or formal requests for information; or violations of the terms and conditions of the license issued to the licensee;

(b) Evidence or proof to support the above;

(c) The level of financial penalty to be imposed; and

(d) The grace period to be allowed to the licensee for challenging the intended penalty (which will not be less than 30 days).

CRA-14.6.9 The licensee may either pay the penalty or object within the above period. The CBB will consider any objection and make a formal resolution within 30 days of receiving the objection. Thereafter, the formal resolution and any accompanying penalties are final and must be paid within 30 days.

CRA-14.6.10 Any financial penalties applied by the CBB as regards the implementation of its requirements set out under Module AML, are without prejudice to the criminal sanctions available to the Bahraini courts under the Decree – Law No. 4 of 2001, with respect to the prevention and prohibition of the laundering of money. As with other financial penalties, the imposition of a financial penalty with regards to breaches of the requirements in Module AML does not prevent the CBB from also using other enforcement measures to remedy the same violation (for instance, a Direction).

Financial Penalties for Date Sensitive Requirements

CRA-14.6.11 This Modules contain specific requirements where licensees must comply with, by a precise date. Where a specific due date is involved, the CBB's financial penalties are based on a per diem basis.

CRA-14.6 Financial Penalties (continued)

CRA-14.6.12 This Section applies to date sensitive requirements for:

a. Reporting requirements included in this Module;
b. Public disclosure requirements included in this Module;
c. The report of the external auditor or a consultancy firm approved by the CBB required as per Paragraph AML-3.3.1B(d) of Module AML;
d. Annual licensing fees required as per Section CRA-1.6, and
e. Conduct of Shareholders' Meetings requirements included in Section HC 10.7.

CRA-14.6.13 Financial penalties related to late filing or other date sensitive requirements are calculated as per the following per diem basis:

(a) For category 1 licensees, the financial penalty for late filing is BD 40 per day;

(b) For category 2 and category 3 licensees, the financial penalty for late filing is BD 60 per day; and

(c) For category 4 licensees, the financial penalty is BD 100 per day.

CRA-14.6.14 The various deadlines for submission of reports and annual fees referred to in this Module are defined:

(a) In terms of a specified number of days or months following a given date, such as the last date of a calendar quarter;
(b) A specified number of days or months after the occurrence of a specific event; or
(c) A specific date.

CRA-14.6.15 In imposing financial penalties for date sensitive requirements, the following criteria apply:

(a) Where the due date falls on a weekend or a holiday as designated by the CBB, the first business day following the weekend or holiday will be considered as being the due date;
(b) Where a due date is not complied with by the end of the day on which it is due, holidays and weekend days are included in the number of days the item is considered late;
(c) For returns and other filings, the date received is the date recorded by the CBB's systems in case of returns filed electronically;
(d) In the case of returns filed in hard copy, the CBB stamp is the date received;
(e) All returns are to be sent to the respective Supervision Directorate and the annual fees to the Accounts Directorate, on or before the due date, to be considered filed on time;
(f) A day ends at midnight in the case of returns that must be filed electronically, or at the close of CBB business day, in the case returns are filed in hard copy; and
(g) An incomplete return, where completeness is determined in relation to the requirements of the relevant instructions and Module BR, is considered 'not filed' until the CBB receives all necessary elements of the return.

CRA-14.6 Financial Penalties (continued)

CRA-14.6.16 The CBB does not require any particular method of delivery for returns and filings that are filed in hard copy. The use of the Bahrain postal services, private courier services or other methods of delivery is entirely at the discretion and risk of the licensee. For the payment of annual fees, licensees must follow the requirements of Form ALF, included under Part B of Volume 6.

CRA-14.6.17 A decision to impose a financial penalty for date sensitive requirements is unrelated to whether the CBB issues a reminder; it is the licensee's responsibility to file and disclose on time as per the requirements of this Module.

Procedures for Financial Penalties

CRA-14.6.18 A written financial penalty notice will be addressed to the Chief Executive Officer or General Manager of the licensee or persons referred to in Paragraph (b) of Article (68 bis 1) of the CBB Law concerned. This written notification will describe the contravention concerned, the CBB's evidence supporting a financial penalty, and the factors justifying the level of penalty proposed. Only an Executive or more senior member of the CBB's management may sign the notification.

CRA-14.6.19 The licensee or persons referred to in Paragraph (b) of Article (68 bis 1) of the CBB Law has 30 days from the notification's date of issuance to submit any objections it wishes to make to the CBB, in writing and addressed to the issuer of the original notification. If the licensee or persons referred to in Paragraph (b) of Article (68 bis 1) of the CBB Law decides not to submit objections, it has 30 calendar days from the notification's date of issuance in which to pay the penalty.

CRA-14.6.20 Should the licensee or persons referred to in Paragraph (b) of Article (68 bis 1) of the CBB Law make representations challenging the proposed penalty, the CBB has 30 days from the issuance of those representations in which to re-examine the facts of the case and its conclusions. If the CBB confirms application of a penalty, payment is required within 30 calendar days of a final notice being issued.

CRA-14.6.21 Failure to pay penalties within the required deadlines will be considered a breach of the CBB's regulatory requirements, and will also result in other measures being considered, as described elsewhere in this Chapter.

CRA-14.6.22 In instances where a licensee anticipates that it will be unable to meet any date sensitive requirements prescribed by the Rulebook, it must provide a written notification to the CBB at least one week prior to the prescribed due date outlining the date sensitive requirements which it will be unable to comply with, along with a well justified reason for the non-compliance.

CRA-14.6 Financial Penalties (continued)

Remedying a Compliance Failure

CRA-14.6.23 Payment of a financial penalty does not by itself absolve a licensee or persons referred to in Paragraph (b) of Article (68 bis 1) of the CBB Law from remedying the compliance failure concerned. The CBB will expect the licensee or persons referred to in Paragraph (b) of Article (68 bis 1) of the CBB Law to address the contravention within a reasonable timescale, to be agreed on a case-by-case basis. Failure to do so will result in other measures being considered.

CRA-14.7 Investigation [This Section was deleted in XX 2022]

CBB Policy

CRA-14.7.1 The CBB uses its own inspectors to undertake on-site examinations of licensees as an integral part of its regular supervisory efforts. In addition, the CBB may commission special investigations of licensees in order to help it assess their compliance with CBB requirements, as contained in Article 121 of the CBB Law. Such investigations may be carried out either by the CBB's own officials, by duly qualified experts appointed for the purpose by the CBB (appointed experts), or a combination of the two.

CRA-14.7.2 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 being considered, as described elsewhere in this Module. This Rule is supported by Article 124(a) of the CBB Law.

CRA-14.7.3 The CBB may appoint an individual or a firm as an appointed expert. Examples of appointed experts are lawyers, audit firms and expert witnesses. The appointment of appointed experts is not necessarily indicative of a contravention of CBB requirements or suspicion of such a contravention. For instance, an appointed expert may be commissioned to provide an expert opinion on a technical matter.

CRA-14.7.4 Appointed experts report in a form and within a scope defined by the CBB, and are solely responsible to the CBB for the work they undertake in relation to the investigation concerned. The report produced by the appointed experts is the property of the CBB (but is usually shared by the CBB with the firm concerned). The cost of the appointed experts' work must be borne by the licensee concerned.

CRA-14.7.5 In selecting an appointed expert, the CBB will take into account the level of fees proposed and aim to limit these to the lowest level consistent with an adequate review of the matters at hand, given the qualifications, track record and independence of the persons concerned. Because the cost of such investigations are met by the licensee, the CBB makes only selective use of appointed experts when essential to supplement CBB's other supervisory tools and resources.

CRA-14.7.6 The CBB may commission reports, which require appointed experts to review information from another company within the reporting licensee's group even where that other company is not itself subject to any CBB requirements.

CRA-14.7.7 Licensees must provide all relevant information and assistance to appointed experts on demand. This Rule is based on Article 123 of the CBB Law.

CRA-14.7.8 Further details on the required report and other aspects related to the role of the appointed expert are contained in Section CRA-11.5.

CRA-14.8 Administration [This Section was deleted in XX 2022]

Legal Source

CRA-14.8.1 Article 136 of the CBB Law empowers (but does not oblige) the CBB to assume the administration of a licensee in certain circumstances. These circumstances are outlined in the above Article and may include the following:
a. The licensee has become insolvent;
b. Its solvency is in jeopardy;
c. Its continued activity is detrimental to the financial services industry in the Kingdom; or
d. Its license has been cancelled.

CRA-14.8.2 Article 139 of the CBB Law provides that where the CBB assumes the administration of a licensee, the licensee concerned may appeal within 10 days to the CBB and, subsequently, the courts, in order to challenge its administration by the CBB.

CRA-14.8.3 Articles 135 to 143 of the CBB Law set down the operating parameters of an administration.

CBB Policy

CRA-14.8.4 The CBB views the administration of a licensee as a very powerful sanction, and will generally only pursue this option if less severe measures are unlikely to achieve its supervisory objectives.

CRA-14.8.5 Although Article 136 of the CBB Law specifies the circumstances in which the CBB may pursue an administration, it does not oblige the CBB to administer a licensee. Faced with the circumstances described, the CBB may pursue other courses of action such as suspension of a license (under Article 131 of the CBB Law), if it considers that these are more likely to achieve the supervisory outcomes sought. Because an administration is likely to send a negative signal to the markets about the status of a licensee, other supervisory actions may in fact be preferable in terms of protecting the interests of those with a claim on the licensee.

CRA-14.8.6 The criteria used by the CBB in deciding whether to seek an administration of a licensee include the following:
(a) The extent to which the interests of the market, its users and those who have a claim on the licensee would be best served by the administration of the license, for instance because of the potential impact on asset values arising from an administration;
(b) The extent to which other regulatory actions could reasonably be expected to achieve the CBB's desired supervisory objectives (such as restrictions on the licensee's operations, including limitations on new business and asset disposals);
(c) The extent to which the liquidity or solvency of the licensee is in jeopardy; and
(d) The extent to which the licensee has contravened the conditions of the CBB Law, including the extent to which the contraventions reflect more widespread or systemic weaknesses in controls and/or management.

CRA-14.8 Administration (Continued)

Procedure for Implementing an Administration

CRA-14.8.7 All proposals for assuming the administration of a licensee are subject to a thorough review by the CBB of all relevant facts, assessed against the criteria outlined in Section CRA-14.8 to CRA-14.8.3.

CRA-14.8.8 A formal notice of administration is issued to the licensee concerned and copies posted in every place of business of the licensee. As soon as practicable thereafter, the notice is also published in the Official Gazette and in one Arabic and one English newspapers in the Kingdom. The term "in administration" should be clearly marked in all the licensee's correspondence and on its website, next to the licensee's name.

CRA-14.8.9 Article 136 of the CBB Law allows a licensee 10 days following the administration taking effect in which to appeal to the CBB. If the CBB refuses the appeal, the licensee has a further 30 calendar days from the date of the refusal in which to lodge an appeal at the courts. So as to reduce the potential damage of an administration order being applied and then withdrawn on appeal, where feasible the CBB will give advance notice to a licensee's Board of its intention to seek an administration, and allow the Board the right of appeal prior to an administration notice being formally served.

CRA-14.9 Cancellation or Amendment of License [This Section was deleted in XX 2022]

Legal Source

CRA-14.9.1 Article 48 of the CBB Law empowers the CBB to cancel or amend a license under certain circumstances. These include cases where a licensee has:
(a) Failed to satisfy its license conditions;
(b) Violated the terms of the CBB Law, CBB Regulations or this Module; or
(c) Failed to start business within six months from the date of the license;
(d) Ceased to carry out the licensed activities permitted; or
(e) Not acted in the legitimate interest of its customers or creditors.

CRA-14.9.2 Article 48(d) of the CBB Law also requires the CBB to give the licensee concerned reasonable time to object to any proposed cancellation or amendment of its license.

CBB Policy

CRA-14.9.3 The CBB generally views cancelling a license as appropriate only in extreme circumstances, when faced with the gravest of contraventions or when left with no other reasonable means of successfully addressing the regulatory failings in question. Cancellation or amendment of a license, however, may also be required in circumstances outside of an enforcement context, for instance because of a change in the business profile of a licensee.

CRA-14.9.4 The criteria used by the CBB in assessing whether to seek cancellation or amendment of a license include:
(a) The extent to which the interests of the market, its users and those who have a claim on the licensee would be best served by the cancellation or amendment of the license;
(b) The extent to which other regulatory penalties could reasonably be expected to achieve the CBB's desired supervisory objectives;
(c) The extent to which the licensee has contravened the conditions of its license and/or the CBB Law, including the seriousness, duration and/or frequency of the contravention(s) concerned, and the extent to which the contraventions reflect more widespread or systemic weaknesses in controls and/or management;
(d) The extent to which the licensee has been involved in financial crime or other criminal conduct; and
(e) The licensee's past compliance record and conduct following the contravention(s).

CRA-14.9.5 When the CBB issues a notice of cancellation or amendment as an enforcement tool, it will only implement the actual change once it is satisfied that there are no longer any regulated activities for which it is necessary to keep the current authorisation in force. Until such time as these activities have been run off or moved to another licensee, the CBB will control these activities through other means (such as taking the licensee into administration or through issuing Directions).

CRA-14.9 Cancellation or Amendment of License (continued)

Procedure for Cancellation or Amendment of License

CRA-14.9.6 All proposals for cancelling or amending a license are subject to a thorough review by the CBB of all relevant facts, assessed against cases and the criteria outlined in Sections CRA-14.9.1, CRA-14.9.2 and Section CRA-14.9.3 to CRA-14.9.5. After being assessed at the Executive Director level, proposals are submitted to H.E. The Governor for approval.

CRA-14.9.7 Once approved within the CBB, a formal notice of cancellation or amendment is issued to the licensee concerned. The notice of cancellation or amendment will describe the factual circumstances of the contraventions concerned, and the CBB's rationale for the proposed cancellation or amendment, as measured against the criteria outlined in Sections CRA-14.9.1, CRA-14.9.2 and Section CRA-14.9.3 to CRA-14.9.5.

CRA-14.9.8 The licensee has 30 calendar days from the date of the notice in which to lodge an appeal. The appeal should be addressed to the Board of the CBB, and copied to H.E. the Governor of the CBB.

CRA-14.9.9 If an appeal is lodged, the Board of the CBB will make a final ruling within 60 calendar days of its date of issuance.

CRA-14.9.10 A licensee may appeal to a competent court within 60 calendar days of the above final ruling for a decision. The court's decision will then be final.

CRA-14.10 ~~Criminal Sanctions~~ [This Section was deleted in XX 2022]

~~Overview~~

~~CRA-14.10.1 The CBB Law provides for a number of criminal sanctions in cases where certain of its provisions are contravened. This Section provides a summary of those sanctions most relevant to licensees, their Directors and employees. What follows is not a complete list of all sanctions provided for in the CBB Law, nor is it a substitute for reading the Law and being fully aware of its provisions.~~

~~CRA-14.10.2 Licensees, their Directors and employees should also be aware of the criminal sanctions provided for under other relevant Bahraini laws, such as the Decree – Law No. 4 of 2001, with respect to the prevention and prohibition of the laundering of money.~~

~~CRA-14.10.3 In all cases to do with criminal sanctions, the CBB can only refer the matter to the Office of Public Prosecutor. The CBB has no authority to apply such sanctions directly without recourse to the courts.~~

~~CBB Policy~~

~~CRA-14.10.4 Because of their criminal status, and their provision for custodial sentences, the sanctions provided for under the CBB Law are viewed by the CBB as very powerful measures, to be pursued sparingly. In most situations, the CBB will seek to address regulatory failures through administrative sanctions, as outlined in preceding Sections, rather than by pursuing the criminal sanctions outlined here.~~

~~CRA-14.10.5 Where, however, the nature of the offence is such that there is strong evidence of a reckless or intentional breach of the CBB Law relevant to the following Articles, then the CBB will usually refer the matter to the Office of Public Prosecutor.~~

~~Articles of CBB Law~~

~~Article 161~~

~~CRA-14.10.6 Article 161 of the CBB Law provides for a penalty of up to BD 1 million, without prejudice to any other penalty prescribed in any other law, in case of any person who breaches the provisions of Resolution No.(16) for the year 2012 issued pursuant to Article 42 of the CBB Law. The Court may also confiscate the proceeds resulting from breaching the Resolution.~~

CRA-14.10 Criminal Sanctions (continued)

Article 163

CRA-14.10.7 Article 163 of the CBB Law provides for a term of imprisonment and/or a fine of up to BD 20,000, without prejudice to any other penalty prescribed in any other law, in case of conviction of a Director, manager, official, agent or representative of any licensee who:

(a) Conceals any records, information or documents requested by the CBB (or any person appointed by the CBB to conduct an investigation or inspection); Provides statements or information in bad faith which do not reflect the actual financial position of the licensee;

(b) Conceals from an external auditor any records, information or documents necessary for auditing the accounts of the licensee; and

(c) Provides in bad faith any misleading or inaccurate statements to an external auditor which do not reflect the actual financial position of the licensee.

Article 169

CRA-14.10.8 Article 169 provides for a term of imprisonment, and/or a fine of up to BD 20,000 for any Director, manager, official or employee, who acts or permits an act in violation of Article 134 of the CBB Law where he knows (or should have known) that the licensee is insolvent.

Article 170

CRA-14.10.9 Part 2 of Article 170 of the CBB Law provides for term of imprisonment and/or a fine not exceeding BD3,000 if any Director, manager, official or employee intentionally obstructs an investigation by the CBB or an investigator appointed by the CBB.

Article 171

CRA-14.10.10 Article 171 of the CBB Law provides for a term of imprisonment and/or a fine not exceeding BD10,000, if any Director, manager, official or employee discloses in bad faith any confidential information relating to a customer of the concerned licensee.

This appendix is part of the requirement specified under CRA-5.8.19 (cyber security)

Appendix -1

CYBER SECURITY INCIDENT REPORTING TEMPLATE

Instructions

1. Licensees are required to report cyber security incident or breach to the CBB on the day of the occurrence of the cyber security incident or breach.
2. Licensees are required to complete and submit the form below via email to the CBB.

Cyber Security Incident Report

1. Contact Information	
Details of the responsible person	
(a) Full Name	
(b) Designation	
(c) Office phone no.	
(d) Mobile no.	
(e) Email address	
Alternate Contact Person	
(a) Full Name	
(b) Designation	
(c) Office phone no.	
(d) Mobile no.	
(e) Email address	
Licensee Details	
(a) Licensee name	
(b) Licensee address	
(c) Type of licensee	
(d) Contact no.	
(e) Email address	
2. Cyber Incident or breach Details	
(a) Date and time of incident or breach	
(b) Details of cyber incident or breach (i) Method of the cyber attack (ii) Duration of the cyber attack	
3. Impact of systems, assets or information	
(a) Affected hardware	
(b) Affected software	
(c) Affected operating system	
(d) Impact to stakeholders	
(e) Geographical location and IP address of attacker	

~~*4.* Resolution of cyber incident or breach~~	
~~(a) What are the immediate remedial actions taken to minimise and mitigate risks from the cyber attack?~~	
~~(b) What is the current status or resolution of this incident or breach?~~ ~~☐ Resolved~~ ~~☐ Unresolved~~	

This appendix is part of the requirement specified under CRA-14.6.2 (Enforcement)

Appendix -2

Methodology for calculating financial penalties

I. Introduction

This appendix sets out the Central Bank of Bahrain's ("CBB") approach on assessing and calculating/determining financial penalties.

The purpose of the financial penalties is to encourage a high standard of conduct and compliance by CBB licensees, thereby reducing risk to their customers and the rest of the financial sector.

The imposition of a financial penalty does not preclude the CBB from also using other enforcement measures to remedy the same violation.

II. The Scope of application

In assessing whether to serve a financial penalty upon a licensee the CBB shall consider the following additional criteria:

(a) The assessment of gain/benefit made or cost avoided and/or the level of risks posed to customers, financial position of the licensee, shareholders, stability of the financial sector and/or the reputation of the Kingdom.

(b) If the licensee made any gain/benefit or avoided any costs by violating the CBB Rules then the gain/benefit and/or the cost avoided will be used as a benchmark for calculating the fine amount subject to BD 100,000 cap for each violation. In addition, the customers impacted must be compensated in full. The scope of this section does not cover penalties for non-compliance with date sensitive requirements of Section CRA-14.6.11 to CRA-14.6.17.

(c) Fit and proper reassessment tests would take place for the approved persons deemed to be responsible for serious or repeated violations at the discretion and judgment of the CBB. The relevant approved person/(s) will be identified based on a review of relevant information including but not limited to the bank's licensee's records before the final decision is made.

(d) Each incident of breaching a Rule (CBB Law, regulations, resolutions, and Rulebook directives) will be considered a stand-alone violation.

(e) If the CBB discovers that one or more breaches had been committed by the licensee in the past and had gone un-detected, then the CBB has the right, at the point of detection, to impose penalties for each of these past breaches.

(f) If the gain/benefit made and/or cost avoided cannot be quantified, then the table below will be used to determine the penalty amount based on the seriousness of violations as determined by the CBB.

(g) The factors used to determine the seriousness of the violation include, but are not limited to, the level of risks posed to the licensee's customers, financial position of the licensee, shareholders, stability of the financial sector and/or the reputation of the Kingdom. The CBB may consider other factors or circumstances as well.

Table 1: Risk Rating of Violation and Related Penalty

Risk Rating		Fine Amount (BD)
1	Low	1,000 to 10,000
2	Medium	10,001 to 50,000
3	High	50,001 to 100,000

III. Internal Assessment by the CBB

In deciding which level of risk is most appropriate (which will then determine the size of the penalty amount in relation to the violation), various factors will undergo comprehensive assessment including but not limited to the following:

1) Impact of the violation;
2) Nature of the violation;
3) Factors showing whether the violation was deliberate; and
4) Mitigating and aggravating factors.

1. Impact of the violation

Factors relating to assessment of the impact of a violation licensee include:

(a) The level of benefit gained or loss avoided, or intended to be gained or avoided, by the licensee as a result of the violation, either directly or indirectly;
(b) The loss or risk of loss, as a whole, caused to customers, investors or other market users in general;
(c) The loss or risk of loss caused to individual customers, investors or other market users;
(d) Whether the violation had an effect on particularly vulnerable people, whether intentionally or otherwise;
(e) The inconvenience or distress caused to customers; and
(f) Whether the violation had an adverse effect on the financial sector and, if so, how serious that effect was. This may include its impact on the confidence in or damage caused to the financial sector. A violation is generally more serious when it causes or may cause extensive financial damage, or when it is likely to be particularly detrimental to investor or customer confidence.

2. Nature of the violation

Factors relating to assessment of the nature of the violation include:

(a) Whether the violation revealed serious or systemic weaknesses in the licensee's procedures or in the management systems or internal controls relating to all or part of the licensee's business;
(b) Whether the licensee's senior management was aware of the violation;
(c) The nature and extent of any financial crime facilitated, occasioned or otherwise attributable to the violation;
(d) The scope for any potential financial crime to be facilitated, occasioned or otherwise occurred as a result of the violation;
(e) Whether the licensee failed to conduct its business with integrity; and
(f) Whether the licensee, in committing the violation, took any steps to comply with CBB Law, regulations, resolutions, Rulebook directives, and the adequacy of such steps.

3. Factors showing whether the violation was deliberate

Factors relating to assessment of whether the violation was deliberate include:

(a) The violation was intentional, in that the licensee's approved person(s), intended or foresaw that the likely or actual consequences of their actions or inaction would result in a violation and they failed to adequately mitigate that risk;

(b) The licensee's approved person(s) knew that their actions were not in accordance with the licensee's internal policies and procedures;

(c) The licensee's approved person(s) sought to conceal their misconduct;

(d) The licensee's approved person(s) committed the violation in such a way as to avoid or reduce the risk that the violation would be discovered;

(e) The licensee's approved person(s) were influenced to commit the violation by the belief that it would be difficult to detect;

(f) The violation was repeated; and

(g) In the context of a contravention of any Rule or requirement imposed by or under CBB law, regulations, resolutions, Rulebook directives, the licensee obtained reasonable professional advice before the contravention occurred and failed to follow that advice. Obtaining professional advice does not remove a person's responsibility for compliance with applicable Rules and requirements.

4. Mitigating and aggravating factors

Mitigation and aggravating factors include:

(a) The conduct of the licensee in bringing (or failing to bring) quickly, effectively and completely the violation to the CBB's attention;

(b) The degree of cooperation the licensee showed during the investigation of the violation. Correspondingly, if the licensee takes a passive stance towards the matter or avoids investigating the matter properly with the CBB, it is likely to increase the penalty payment and/or imposing other enforcement measures.

(c) Where the licensee's approved person(s) were aware of the violation or of the potential for a violation, whether they took any steps to stop the violation, and when these steps were taken;

(d) Any remedial steps taken by the licensee prior to the discovering of such violation by the CBB; for example, identifying whether customers or investors or other market users suffered loss and compensating them where they have; correcting any misleading statement or impression; taking disciplinary action against staff involved (if appropriate); and taking steps to ensure that similar problems do not arise in the future;

(e) Whether the licensee had previously been told about the CBB's concerns in relation to the issue, either by means of a written formal warning/notice and/or Direction;

(f) Whether the licensee had previously undertaken not to perform a particular act or engage in a particular behavior;

(g) The previous disciplinary record and general compliance history of the licensee;

(h) Action taken against the licensee by other domestic or international regulatory authorities that is relevant to the violation in question.

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 in the Kingdom of Bahrain 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:**

(i) Equivalent of an equity security: where it confers or represents ownership interest in a company or gives entitlement to share in the issuer's profit; or

(ii) 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 or may be lent to the issuer by the digital token holder, its maturity is fixed, are 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 should be considered as a security, the CBB shall, amongst others, take into consideration the following:

(i) 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?
(ii) Does the digital token represent a monetary claim on the digital token issuer?
(iii) Is the digital token transferable?
(iv) Does it confer decision power on the project of the digital token issuer?

CRA-15.1.5 The CBB is mindful of the fact that various types of digital tokens are currently being offered. The guidance provided is indicative and not exhaustive and, the CBB reserves the right to 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:

CRA-15.1 Digital Token Offerings (continued)

(a) Utility tokens: A utility token shall be treated as 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 a security.
A utility token shall not be treated as a security if the sole purpose is to confer digital access rights to an application or 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 missing.

(b) Asset tokens: An asset token shall be treated as a security under following conditions:
a. The asset token gives right to financial entitlement and exhibits features of either bonds or equity securities: a bond if the entitlement is a predetermined cash flow; an equity security if the entitlement is a share in profit.
b. The asset token gives right to an entitlement in kind, and the holder gets decision power into the project, the asset token shares important characteristic with equity securities.

Initial Assessment

CRA-15.1.6 Potential digital token issuers seeking to undertake 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 company and description of the project, to the CBB to determine suitability of the digital token for issuance. The CBB will guide the potential digital token issuer on the regulatory requirements that shall apply.

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, dilute or be contrary to the interests of the holders of the digital tokens or public investors in general.

CRA-15.1.8 The CBB may refuse to grant its approval, postpone granting such approval, or impose additional terms and conditions, if the CBB deems that the market condition or circumstances justifies such action.

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 who is not publicly listed on a stock exchange;

(b) The digital token issuer must have a minimum paid up capital of BD 50,000 or equivalent amount in other currency, and maintain a minimum shareholders' equity of BD 50,000 at all times;

(c) The digital token issuer must ensure no conflict of interest arises during either the issuing of digital tokens;

(d) The digital token issuer must appoint an eligible CBB licensed retail bank to deposit all funds raised through the digital token issue in a separate escrow account;

(e) The digital token issuer must protect and act in the interests of digital token holders and provide equal treatment to all digital token holders;

(f) The digital token issuer must adhere to the offering and issuing timetable contained in the whitepaper, or as amended upon the CBB's approval;

(g) The maturity period of a digital token exhibiting characteristic of bond or debt security must not exceed 5 years;

(h) For any single offering of digital token, the digital tokens must have identical terms and conditions of issuance including having same price;

(i) Funds that can be raised by a digital token issuer through digital token offering must be limited to 5 times the shareholder's equity or BD 5 million, whichever is lower; and

(j) 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 1 month.

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.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

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 members must not sell, transfer or assign more than 50% of their initial equity holding for a period of 3 years, starting from the date of 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 staff of the digital token issuer. The cooling-off period must be no fewer 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 his/her 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 are free to set a higher soft cap.

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 refund made, the failure to reach the soft cap and cancellation of the digital token offer to the CBB.

CRA-15.1 Digital Token Offerings (continued)

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 provision, among others, on the schedule of release of proceeds (if stated in the whitepaper), the progress report that will be required before each release of proceed, and that the digital token advisor will return the said proceed 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 abandoned by the digital token issuer.

CRA-15.1.19 The escrow account agreement 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 has been abandoned by the digital token issuer with notification to the CBB.

CRA-15.1.20 If the digital token issuer abandons the project before completion, the appointed digital token advisor must:

(a) Immediately notify the CBB regarding the abandonment of the project by the digital token issuer and the reason behind such abandonment; and

(b) Within 5 business days from the date of notifying to the CBB, individually notify each investor about the abandonment of the project by the digital token issuer and refund the remaining proceed under its care on pro-rata basis to the investor 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.

CRA-15.1 Digital Token Offerings (continued)

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 may be 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 approve the application in 30 working days subject to receiving the documents complete in all aspects.

CRA-15.1.25 **The CBB's approval for an offer of digital token does not imply that it has approved the appropriateness of the digital token issuer's project or authenticated the financial and technical information presented in the whitepaper.**

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 offering period, or before the amount 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 any requirement under the CBB Law, requirements of this Module or any other applicable Modules issued by the CBB;

(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;

(d) There is a concern with the digital token issuer's corporate governance record or with the integrity of any of the digital token issuer's directors and senior management; or

(e) The CBB has reason to believe that the approval of the application would be contrary to public interest.

CRA-15.1 Digital Token Offerings (continued)

Documentation Requirements

CRA-15.1.28 A digital token issuer, through its appointed digital token advisor, must register with the CBB the following documents:

(a) A draft whitepaper in accordance with 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;
(e) Documents proving the establishment of an arrangement ensuring monitoring and safeguarding of the funds collected through the digital token offering in accordance with Paragraph CRA-15.2.10;
(f) All marketing material related to the digital token offering; and
(g) 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).
(h) 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).
(i) A copy of the duly signed declaration by the legal advisor for the digital token offer, based on a due diligence exercise of all relevant legal conditions, facts and arrangements including enforceability of the rights against the digital tokens, as appropriate (Appendix CRA-4);
(j) 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; and
(k) Any other information as required by the CBB.

Registration of Whitepaper

CRA-15.1.29 Once the whitepaper and other documents are approved by the CBB subject to changes, the final corrected copy must be registered with the CBB within 2 business days.

CRA-15.1 Digital Token Offerings (continued)

Contents of the Whitepaper

CRA-15.1.30 The whitepaper must contain, either in Arabic or English language, all the information concerning the digital token issuer and the planned digital token offering needed to 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 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 digital token holders' claims in the event of insolvency or liquidation;
(f) A detailed description of the digital token offering, including but not limited to:
    (i) number of digital tokens to be issued;
    (ii) digital token issue price;
    (iii) subscription terms and conditions;
    (iv) minimum amount necessary to carry out the project and the maximum amount of the offering; and
    (v) the subsequent use and application of the proceeds thereafter illustrated in a scheduled timeline for drawdown and utilisation of proceeds ("schedule of proceeds");
(g) The technical specifications of the digital token;
(h) 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;
(i) A detailed description on the determination of the accounting and the valuation treatments for the digital token including all valuation methodology and reasonable presumptions adopted in such calculation;

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.1 Digital Token Offerings (continued)

(j) The allotment policy for the digital tokens;
(k) 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;
(l) Detailed description of the sustainability and scalability of the underlying business or project;
(m) Detailed description of the financial, technical, legal and commercial due diligence and market feasibility undertaken on the project;
(n) Audited financial statements of the digital token issuer for the stipulated period; and
(o) 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, not misleading, must be presented in a concise and comprehensible manner and must not include any promotional jargon to excite rather than to inform.

CRA-15.1.33 The whitepaper must be prepared in accordance with the template provided in CRA Appendix-1.

CRA-15.1.34 The CBB, prior to approving an application for offering of digital tokens, shall check whether the information provided in the whitepaper is complete and comprehensible. The whitepaper shall be drawn up by the digital token issuer under the guidance of the digital token advisor and 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 Arabic and English language.

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;

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.1 Digital Token Offerings (continued)

(b) It must ensure that the funds collected are deposited in a 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 three months from the date of notification of the CBB approval. After this period no person shall offer digital tokens based on such whitepaper, unless approved by the CBB.

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, under the following circumstances:

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 significant change affecting a matter disclosed in the whitepaper;

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.1 Digital Token Offerings (continued)

c) The whitepaper contains a statement or information that is false and 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 three-month time limit referred to in Paragraph CRA-15.1.39.

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/clauses 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-15.1.44 The CBB shall give its approval on the supplementary whitepaper within 15 working days provided the digital token issuer furnishes necessary information complete in all aspects.

CRA-15.1.45 The supplementary whitepaper must be published and disseminated in accordance with the same procedure 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 fewer 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. No fee must be charged to the investor for the refund.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.1 Digital Token Offerings (continued)

Dissemination of whitepaper

CRA-15.1.47 Upon approval by the CBB, the whitepaper must be made available to public 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 website 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 can only be disseminated after obtaining the CBB's approval.

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 subscribers can obtain the whitepaper approved by the CBB by specifying the name of the website(s) where it can be found;
(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 non-misleading;
(e) disclose the risks related to the digital token offering;
(f) contain information that is consistent with and does not contradict 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.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.1 Digital Token Offerings (continued)

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 prior approval of the CBB, in such instances where the marketing material is not in line with the changes made through the supplementary whitepaper.**

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 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.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.2 Digital Token Issuers Obligations

General Obligations

CRA-15.2.1 The digital token issuers must meet the following requirements:

(a) Appoint and retain 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) A digital token issuer must 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 for these risks to ensure compliance with its obligations relating to anti-money laundering and terrorist financing;
(e) A digital token issuer must provide to the CBB any information or assistance as the CBB deems necessary relating to the digital tokens;
(f) A digital token issuer must retain all relevant documents and agreements related to the digital token offering for a period of five (5) years; and
(g) A digital token issuer is 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 or an equivalent governing body. 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 its obligations under this Module as well as with the CBB Law, rules and regulations.

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.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

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 its investors;
(b) exercise reasonable care, skill and diligence;
(c) exercise the powers they have diligently and in line with applicable law and must 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 functionaries and must be satisfied that they are performing their functions in accordance with their contractual obligations;
(f) identify and manage the risks of the digital token issuer and his activities;
(g) monitor, on an ongoing basis compliance with the requirements of CBB Law, rules and regulations including the requirements of this Module and other applicable Modules;
(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 appropriate 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 personnel:

(a) have access to 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 senior management person leaves the organisation or is removed or replaced, such a change must be immediately disclosed to the digital token advisor and the investors.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.2 Digital Token Issuers Obligations (Continued)

DRO-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 company;

(b) They are not 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, dishonesty, mismanagement of a company;

(d) They have not had any civil enforcement action initiated against them in any court of law, whether within or outside Bahrain;

(e) They have not:

(i) been convicted, whether within or outside Bahrain, of an offence involving fraud or other dishonesty or violence or the conviction of which involved a finding that he acted fraudulently or dishonestly;

(ii) been convicted of an offence under the securities laws or any law within or outside Bahrain relating to the capital market;

(iii) contravened any provision made under any law whether within or outside Bahrain appearing to the CBB to be enacted for protecting members of the public against financial loss due to dishonesty, incompetence or malpractice by persons concerned in the provision of financial services or the management of companies or against financial loss due to the conduct of discharged or undischarged bankrupts;

(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 on his 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 his 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 to the CBB 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.

Fund Monitoring and Safeguarding Arrangement

CRA-15.2.10 Digital token issuers must have in place a fund monitoring and safeguarding arrangement for the funds raised through the digital token offering which must include

(a) Establishing an escrow account arrangement with a licensed retail bank based in Kingdom of Bahrain. The escrow account arrangement must address criteria for withdrawal and transfer of funds. The fulfilment of the criteria must be verified by the digital token advisor prior to release of funds; and
(b) The procedures for collection and management of the funds including procedures for the utilisation, refund and release of funds.

Digital Token Advisor Requirements

CRA-15.2.11 Before, appointing a digital token advisor, the digital token issuer must 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 must consider the following:

(a) Historical records and prior performance;
(b) Have adequate systems, controls and resources to discharge its obligations under the CBB rules in this regard; and
(c) Suitably experienced and qualified employees having adequate knowledge and professional expertise to discharge its obligations.

CRA-15.2.12 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.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.2 Digital Token Issuers Obligations (Continued)

Repurchase of Digital Tokens

CRA-15.2.13 If a digital token issuer has disclosed a digital token repurchase mechanism in the whitepaper, it may, after its digital tokens have been traded on the crypto-asset exchange for a full year, by agreement of a majority of the directors in attendance at a board meeting attended by at least two-thirds of the directors, carry out a repurchase (buyback) of its digital tokens on the crypto-asset exchange, and must complete the execution of the buyback within 2 months from the day of making the public disclosure about the repurchase (buyback).

CRA-15.2.14 A digital token issuer must immediately cancel the digital tokens that it acquires under the digital token repurchase plan.

CRA-15.2.15 After the digital token issuer has repurchased digital tokens under Paragraph CRA-15.2.13, if the quantity of outstanding digital tokens is lower than 10% of the originally issued quantity, the digital token issuer must publicly announce the termination of trading of the digital token.

Periodic Reporting Requirements

CRA-15.2.16 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-15.2.18 and publish it on the digital token advisor's platform.

CRA-15.2.17 A digital token issuer must prepare and publish a report, in accordance with CRA-15.2.18, 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-15.2.18 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 will be applied to manage and resolve such problems;
(e) risks facing the underlying business or project and mitigation; and
(f) unaudited quarterly financial statements reviewed by the external auditor for quarterly reporting and audited annual financial statements for annual reporting.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.2 Digital Token Issuers Obligations (Continued)

CRA-15.2.19 **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-15.2.20 **A copy of the quarterly report and annual report referred to in Paragraph CRA-15.2.6 and CRA-15.2.7 must be filed with the CBB no later than the date of its publication.**

Disclosure of Material Information

CRA-15.2.21 **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-15.2.22 For the purposes of CRA-15.2.1, the following events should 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 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) Signing, 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 transactions, with a material effect on the finances or business 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;
(j) Change in 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

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.2 Digital Token Issuers Obligations (Continued)

(m) Announcement of suspension or termination of trading of the digital tokens on the crypto-asset exchange.

CRA-15.2.23 **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-15.2.24 **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 provisions under which the information was originally disclosed.**

Power of the CBB to issue Direction

CRA-15.2.25 **The CBB may at any time issue a direction to the digital token issuer, the digital token issuer's Board and/or its senior management or any other related person, must be complied with, if the CBB:**

(a) is of the view that it is necessary or expedient for the:

(i) purposes of ensuring fair and orderly market; or

(ii) purposes of the protection of the holder of digital token, or in the public interest; or

(b) is of the opinion that the underlying project or business is no longer viable or sustainable.

CRA-15.2.26 A direction issued under Paragraph CRA-5.2.25 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 or digital token as the CBB deems necessary;

(e) to give effect to any requirement of the applicable laws, rules and regulations; or

(f) on any other direction 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 crypto-asset exchange acting as a digital token advisor to a digital token issuer.

CRA-15.3.2 Digital token issuers must appoint and have at all times a crypto-asset exchange (Category-4, CRA Licensee) who shall act as an advisor (digital token advisor) and ensure that the digital token issuer satisfies all requirements as prescribed under the CBB Law, rules and regulations.

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 the digital token advisor:

(a) has ownership interest in the digital token issuer or any other company within the digital token issuer's group;

(b) 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, partner or employee of the appointed digital token advisor or another entity in the appointed digital token advisor 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.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 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 and applicable rules and regulations;

(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) submit to the CBB all required information and documentation including the documents required for assessment of the digital token offer, in a timely manner;

(e) carry out due diligence on a digital token issuer including:

(i) understanding and verifying the business 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 of 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; and

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, clear, not misleading and there are no material omissions.

CRA-15.3 Role and Responsibilities of Digital Token Advisor (Continued)

(f) 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

(g) 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 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;

(h) disclose any information or provide any document to the CBB as it may require;

(i) ensure that all disclosures are fair, accurate, clear and not misleading; and

(j) 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;

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

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 terms and conditions imposed by the CBB, any provisions of the CBB laws, other applicable rules and regulations including provisions of this Module; and

(b) any material adverse change to the digital token issuer's 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 investors (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 must 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.

CRA-15.3 Role and Responsibilities of Digital Token Advisor (Continued)

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 investor.**

Record of Investors 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 records of investors and any monies or digital tokens held in relation to the investors.**

CRA-15.3.14 A digital token advisor must ensure that records pertaining to (i) register of initial digital token holders, (ii) current digital token holders and (iii) the "self-declaration form" submitted by expert investor and retail investor are 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 -8 of this Module.**

CRA-15.3.16 **A digital token advisor must ensure digital tokens held under 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 based 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 condition before releasing the funds, provided that the additional condition serve the interest of the investors.

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 listed on a crypto-asset exchange can be conducted either by:

(a) Operating a conventional market wherein buyers and sellers are allowed to trade in a manner similar to that followed in conventional securities exchanges and this includes, amongst other, that 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 crypto-asset exchange 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 for trading on both types of markets i.e. conventional securities exchange type market and over-the-counter trading market.

Over-the-counter Trading

CRA-15.4.3 A crypto-asset exchange 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 A crypto-asset exchange 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 A crypto-asset exchange undertaking over-the-counter trading of digital tokens must open a dedicated account at a licensed bank for the collection and payment of funds.

MODULE	CRA: Crypto-asset
CHAPTER	CRA-15 Digital Tokens

CRA-15.4 Trading and Settlement of Digital Tokens (continued)

CRA-15.4.7 A crypto-asset exchange engaging in over-the-counter trading of digital tokens must provide two-way, buy and sell, quotes.

CRA-15.4.8 A crypto-asset exchange, 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 crypto-asset exchange 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 A crypto-asset exchange 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, a crypto-asset exchange 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 crypto-asset exchange, 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 A crypto-asset exchange undertaking over-the-counter trading must adhere to Conduct of Business Obligations as stipulated in Section CRA-12 of this Module.