Crypto-asset Platform Operators
Module CPO

MODULE	CPO: Crypto-asset platform operator
CHAPTER	CPO-A Table of Contents

Date Last Changed

Date Last Changed

Date Last Changed

MODULE	CPO: Crypto-asset platform operator
CHAPTER	CPO-A Introduction

CPO-A.1 Purpose

Executive Summary

CPO-A.1.1 The purpose of this Module is to provide the CBB's Directive concerning dealing in crypto-assets as principal, as agent and as a custodian 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').

CPO-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;

Legal Basis

CPO-A.1.3 **This Module contains the CBB's Directive (as amended from time-to-time) relating to crypto asset platform operators as defined in the Rulebook and is issued under the powers available to the CBB under Article 38 of the CBB Law. Crypto asset platform operators must also comply with the relevant Modules of the Rulebook Volume 6.**

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

CPO-A.2 Module History

CPO-A.2.1 This Module was first issued in [MONTH] 2018. 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.

Effective Date

CPO-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.**

CPO-B.1 Overview

CPO-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.

CPO-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 and the powers under the CBB Law for inspections and access.

MODULE	CPO: Crypto-asset platform operator
CHAPTER	CPO-1 Licensing

CPO-1.1 License for crypto-asset platform operators

1.1.1. **No person may market or undertake the activities, by way of business, within or from the Kingdom of Bahrain of a crypto asset platform operator without obtaining a license from the CBB.**

1.1.2. **For the purposes of paragraph 1.1.1, the activities of a crypto asset platform operator mean providing any or a combination of the following types of services:**

(a) dealing in accepted crypto assets as principal;
(b) dealing in accepted crypto assets as agent;
(c) safeguarding, storing, holding, maintaining custody of or arranging custody on behalf of clients for accepted crypto assets.

1.1.3. **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 1.1.2 for commercial gain;
(b) Holding oneself out as willing and able to provide the services specified in paragraph 1.1.2; or
(c) Regularly soliciting other persons to engage in providing the services specified in paragraph 1.1.2.

1.1.4. If any 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. Dealing in crypto-assets shall mean exchanging accepted crypto-asset for fiat currency or exchanging fiat currency for accepted crypto-assets

1.1.5. 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.

CPO-1.1 License for crypto-asset platform operators (continued)

1.1.6. 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.

Exclusions

1.1.7. **The following activities does not constitute regulated crypto-asset service:**

(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;

(c) the transmission of crypto assets; or

(d) a loyalty programmes.

1.1.8. **Persons wishing to be licensed to undertake the activities of a crypto asset platform operator must apply in writing to the CBB.**

1.1.9. **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.

1.1.10. 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.

CPO-1.1 License for crypto-asset platform operators (continued)

1.1.11. Detailed rules and guidance regarding information requirements and processes for licenses can be found in Section CPO-1.2. As specified in Paragraph CPO-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.

1.1.12. **All applicants seeking a crypto-asset platform operator must satisfy the CBB that they meet, by the date of grant of license, the minimum criteria for licensing, as contained in Chapter CPO-2. Once licensed, crypto-asset platform operator must maintain these criteria on an on-going basis.**

Combining Regulated Crypto-asset Services

1.1.13. 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.

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

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

CPO-1.2 Application for License

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 CPO-1.2.4, unless otherwise directed by the CBB.**

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

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.

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 CPO-1.7.2) in the proposed licensee;**
- **(c) A comprehensive business plan for the application, addressing the matters described in Rule CPO-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;**

CPO-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 (j) or (k) 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.

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 CPO-1.2.4 above.

CPO-1.2 Application for License (continued)

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.

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 investment activities or are incidental to those.

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.

1.2.9 Any material changes or proposed changes to the information provided to the CBB in support of an authorisation application that occurs prior to authorisation must be reported to the CBB.

CPO-1.2 Application for License (continued)

1.2.10 Failure to inform the CBB of the changes specified in Rule CPO-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 CPO-2.8.2.

Licensing Process and Timelines

1.2.11 By law, the 60 days' time limit referred to in Paragraph CPO-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 CPO-1.2.4 have to be provided, before the CBB may issue a license.

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

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 CPO-1.2.4. This draft application should contain at least items in Rule CPO-1.2.4(a); Rule CPO-1.2.4(b), with respect to proposed Directors (but not necessarily senior management); Rule CPO-1.2.4(c); Rule-CPO-1.2.4(d); and Rule CPO-1.2.4(g) to Rule CPO-1.2.4(m) inclusive.

1.2.14 On the basis of the information specified in Paragraph CPO-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.

CPO-1.2 Application for License (continued)

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 CPO-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.

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).

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 Central Bank 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.

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 CPO-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).**

CPO-1.2 Application for License (continued)

Granting or Refusal of License

1.2.19 To be granted a license, an applicant must 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.

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.

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

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.

CPO-1.2 Application for License (continued)

Readiness Assessment

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.**

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.**

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

1.2.26 **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 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 1.2.9;**
- **(j) A copy of the commercial registration certificate in Arabic and in English from the Ministry of Commerce, Industry and Tourism;**

CPO-1.2 Application for License (continued)

(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.

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.

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

CPO-1.3 Cancellation of License

Voluntary Surrender of a License

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.

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

1.3.3 Failure to comply with Rule CPO-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

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.

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.

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.

MODULE	CPO: Crypto-asset platform operator
CHAPTER	CPO-1 Licensing

CPO-1.4 Publication of the Decision to Grant or Cancel a License

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.

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

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.

MODULE	CPO: Crypto-asset platform operator
CHAPTER	CPO-1 Licensing

CPO-1.5 Licensing Application Fees

1.5.1 Applicants seeking a 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.

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

CPO-1.6 Annual License Fees

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.**

1.6.2 The relevant fees are specified in Rule CPO-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.

1.6.3 **The variable annual license fee payable by licensees is 0.25% of their relevant operating expenses, subject to a minimum of BD 2,000 and a maximum of BD 6,000.**

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 1.6.5.**

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.**

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.

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.

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.**

MODULE	CPO: Crypto-asset platform operator
CHAPTER	CPO-1 Licensing

CPO-1.6 Annual License Fees (continued)

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.

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 floor amount of BD 300.

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).

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.

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.

CPO-1.7 Approved Persons

General Requirements

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 CMM-1.7.3 and Paragraph CMM-1.7.4.

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).

1.7.3 In the case of Bahraini crypto-asset platform operator, 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 Modules MIR.

1.7.4 In the case of overseas crypto-asset platform operator, prior approval is required for controlled functions (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.

Basis for Approval

1.7.5 For the purposes of Paragraph CPO-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.

CPO-1.7 Approved Persons (continued)

1.7.6 Approval under Paragraph CPO-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.

Cancellation of Approved Person Status

1.7.7 **In accordance with Paragraphs MIR-3.4.11 of Module MIR and CPO-10.2.14, 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.**

1.7.8 The explanation given for any such changes should simply 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.

1.7.9 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.

1.7.10 **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).**

CPO-1.7 Approved Persons (continued)

1.7.11 The fact that a person may have 'Director' in their job title does not of itself make them a Director within the meaning of the definition noted in Paragraph CPO-1.7.10. 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 CPO- 1.7.10.

1.7.12 **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.**

1.7.13 **The Chief Executive or General Manager of the licensee:**

(a) Should 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.

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

MODULE	CPO: Crypto-asset platform operator
CHAPTER	CPO-1 Licensing

CPO-1.7 Approved Persons (continued)

1.7.15 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.

1.7.16 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.

1.7.17 Licensees must designate an employee, of appropriate standing and resident in Bahrain, as compliance officer. The duties of the compliance officer include:
(a) Having responsibility for oversight of the licensee's compliance with the requirements of the CBB; and
(b) Reporting to the licensee's Board in respect of that responsibility.

MODULE	CPO: Crypto-asset platform operator
CHAPTER	CPO-2 Licensing Condition

CPO-2.1 Condition 1: Legal Status

2.1.1 The legal status of a licensed crypto-asset service licensee must be:
(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.

2.1.2 Where the application is for establishing a branch of an overseas crypto-asset platform operator, 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.

CPO-2.2 Condition 2: Mind and Management

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 exchanger licensees must maintain a local management presence and premises in the Kingdom appropriate to the nature and scale of their activities.

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

2.2.3 Overseas crypto-asset platform operators must seek the CBB's prior approval if some of its controlled functions are not resident outside Bahrain.

CPO-2.3 Condition 3: Substantial Shareholders

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

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.

MODULE	CPO: Crypto-asset platform operator
CHAPTER	CPO-2 Licensing Condition

CPO-2.4 Condition 4: Board and Employees

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.

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

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.

CPO-2.5 Condition 5: Financial Resources

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 CPO-3.

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.

CPO-2.6 Condition 6: Systems and Controls

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 CPO-5 (Technology Governance and Cyber Security), Chapter CPO-6 (Risk Management) and the requirements of Module HC (High-level Controls) of the CBB Rulebook Volume 6.

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.

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.

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.

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.

2.6.6 Licensees providing custody services specified in paragraph CPO-1.1.2 (c), must segregate the personnel, systems and controls to avoid conflicts of interest with activities undertaken under CPO-1.1.2 (a) and (b).

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.

CPO-2.7 Condition 7: External Auditor

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.

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

CPO-2.8 Condition 8: Other Requirements

Books and Records

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 platform operator, 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

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 CPO-4.**

Additional Conditions

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

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.

CPO-3.1 General Requirements

Obligation to Maintain Adequate Capital

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.

3.1.2 Licensees undertaking the services of a crypto asset platform operators must maintain, at all times, a minimum capital requirement comprising paid-up share capital, unimpaired by losses, of not less than BD 500,000 plus any additional required capital pursuant to paragraph CPO-3.1.3 and CPO-3.2.1.

3.1.3 In addition to the minimum capital requirements specified in CPO-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.

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:

(i) the composition of the licensee's total assets, including the position, size, liquidity, risk exposure, and price volatility of each type of crypto asset;
(ii) the composition of the licensee's total liabilities, including the size and repayment timing of each type of liability;
(iii) the actual and expected volume of the licensee's crypto asset business activity;
(iv) the liquidity position of the licensee;
(v) the types of products or services to be offered by the licensee.

3.1.5 The initial capital may not be reduced or withdrawn by shareholders from the retail bank at which it is held, without the necessary prior written approval of the CBB.

3.1.6 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.

CPO-3.2 Key Requirements

3.2.1 Crypto asset platform operators dealing in crypto assets as principal and thereby taking proprietary positons in crypto assets shall ensure that the positions are matched at all times by paid-up share capital, retained earnings and unencumbered reserves after taking into account all other assets on their balance sheet.

3.2.2 Overseas crypto-asset platform operator 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 platform operator must ensure compliance with the minimum capital requirements specified in Rule CPO-3.2.2.

3.2.3 As specified in Article 57(a)3 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.

CPO-3.3 Additional Requirements

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.**

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

CPO-4.1 General Obligations

4.1.1 In the course of undertaking regulated crypto-asset services, licensees 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 is sufficient and appropriate records, books and systems in place to record all transactions and maintain an audit trail;

CPO-4.1 General Obligations (continued)

(o) Have an operating manual and internal policies;

(p) Provide to the CBB, for its review and comment, at least 5 business days prior to publishing in the press, the draft agenda for any shareholders' meetings referred to in CPO-4.1.1 (u);

(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 CPO-4.1.1(u), 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 assrt services requirements. The crypto asset compliance policy must reflect a clear comprehension and understanding of compliance responsibilities.

CPO-4.2 Auditors and Accounting Standards

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.

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

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

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.

CPO-4.3 Accepted Crypto-assets

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.

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, including market capitalization, 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.

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

(a) Market Capitalisation: A market capitalisation in excess of US$ 4 billion. The CBB does not prescribe the source for calculating the market capitalisation of a crypto-asset and will consider certain recognised sources, as may be available from time to time.

(b) 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;

(c) 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;

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

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

(f) 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;

CPO-4.3 Accepted Crypto-assets (continued)

(g) 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

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

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.

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.

CPO-4.4 Eligible Investors

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.

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 21 years of age.

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.

4.4.4 Clients must not undertake transactions in accepted crypto assets as agents (acting on behalf of a third party). 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.

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

4.4.6 The bank account details (designated bank account) provided by the client at the time of registration must be used for the purpose of transfer of funds between the client and the licensee as set out under Rules CPO-7.1.5 and CPO-7.1.6. Licensees must register only one bank account as a designated bank account.

CPO-4.5 Client Protection

Segregation and Handling of Clients' Assets

4.5.2 Licensees undertaking regulated crypto-asset service 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 Rules MIR-4.7.9 and MIR-4.7.14.

Client Money

4.5.3 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.

4.5.4 Client money must be received by the licensee directly into a client bank account.

Settlement of Funds and Accepted Crypto-assets

4.5.5 The settlement for transactions in accepted crypto-assets must be done within 24 hours of the receipt of order from the client.

4.5.6 For the purposes of CPO-4.5.5, a licensee must transfer the funds, due to the client or held on behalf of the client, from the client bank account to the designated bank account of the client within the settlement of funds timeline (24 hours) set out in CPO-4.5.5.

Risk Disclosure to Clients

4.5.7 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;

CPO-4.5 Client Protection (continued)

(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.

Disclosure of General Terms and Conditions

4.5.8 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.

CPO-4.5 Client Protection (continued)

Disclosure of the Terms of Transactions

4.5.9 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

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

Confirmation Note

4.5.11 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;

4.5.12 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 CPO- 4.5.11.

CPO- 4.5 Client Protection (continued)

Prevention of Fraud

4.5.13 Licensee 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.

Client Agreements and Statements

4.5.14 Licensees must not carry out a regulated crypto-asset service where this involves service to a client as mentioned under Paragraph CPO-1.1.11 unless there is a client agreement entered into between the licensee and the client containing the key information specified in Rule CPO-4.5.15.

4.5.15 The client agreement referred to in Rule CPO-4.5.14 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 CPO-4.5.7 and disclosure of general terms and conditions referred to in Rule CPO-4.5.8.

CPO-4.6 Marketing and Promotion

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.

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 Platform Operator.

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.

4.6.4 In all advertising and marketing materials, licensees must comply with all disclosure requirements under CBB Law, rules and regulations.

CPO-4.7 Complaints

4.7.1 Licensees must establish and maintain written policies and procedures to fairly and timely resolve complaints.

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;

4.7.3 Licensees must notify to the CBB any change in their complaint policies or procedures within seven days.

Reporting of Complaints

4.7.4 Licensees must submit to the Consumer Protection office 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.

4.7.6 Where no complaints have been received by the licensee within the quarter, a 'nil' report should be submitted to the Consumer Protection office at the CBB.

CPO-4.8 Professional Indemnity Coverage

Key Provisions

CPO-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.**

CPO-4.8.2 **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 a quarterly basis. Additionally, they must provide, upon request, evidence to the CBB of the coverage in force.**

CPO-4.8.3 **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.**

CPO-4.8.3 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.

CPO-4.8.4 Upon written application to the CBB, the requirement in Rule CPO-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.

CPO-4.8.5 **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.**

CPO-4.9 Other Obligations

Obligation to Maintain Proper Records

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

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

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.

CPO-4.10 Matters Requiring Approval of CBB

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

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.

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.

4.10.4 To facilitate the prior approval required under Paragraph CPO-4.10.3, licensees subject to Paragraph CPO-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 CPO-3 (Minimum Capital Requirements) and the liquidity position of the licensee.

CPO-5.1 General Requirements

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).

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.

CPO-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.

CPO-5.2 Maintenance and Development of Systems

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

5.2.1 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.

5.2.2 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.

5.2.3 For the purposes of Rule-5.2.2, the use of version control software which allows for the accurate timestamping and identification of the user responsible for relevant changes must be considered.

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

5.2.5 Licensees must have an annual third-party audit of their IT infrastructures and core systems including penetration testing undertaken by a reputable third party cyber security consultants. The third-party audit report including the recommendations and areas of concerns must be submitted to the CBB. The third-party audit report must also include the areas of concerns identified by the licensee during the IT System audit as set out under CPO-5.9.5 and the measures taken by the licensee to mitigate those concerns.

CPO-5.3 Security Measures and Procedures

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.

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.

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.

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.

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.

5.3.6 Licensees must conduct regular (at least annually) security tests of their systems, network, and connections.

CPO-5.4 Cryptographic Keys and Wallet Storage

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.

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.

5.4.3 Crypto currencies that do not need to be immediately available should be held off line, in a 'cold wallet' to the extent feasible. Below is a non-exhaustive list of some of the measures that licensees should consider.

Password protection and encryption

5.4.4 Both hot and cold wallets should be password protected and encrypted. The key storage file that is held on the online or offline device should 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).

5.4.5 Licensees should consider the use of multi-signature wallets (e.g., where multiple private keys are associated with a given public key and a subset of these private keys, sometimes held by different parties, are required to authorise transactions). Noting that there is no way to recover stolen or lost private keys unless a copy of that key has been made, multi-signature wallets may offer more security because an user can still gain access to its crypto-assets when two or more Private Keys remain available.

Off Line Storage of Keys

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

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 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.

CPO-5.4 Cryptographic Keys and Wallet Storage

Password Deliver Key

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

CPO-5.5 Origin and Destination of Crypto-asset

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.

CPO-5.6 Planned and Unplanned System Outages

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.

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.

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

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

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

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.**

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.**

CPO-5.8 Cyber Security

General Requirements

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 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.

Roles and Responsibilities of the Board

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.

5.8.3 In discharging its oversight functions, the board must:

(a) ensure that the licensee's policies and procedures 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;

CPO-5.8 Cyber Security (continued)

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

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.

CPO-5.8 Cyber Security (continued)

Cyber Security Risk Policy

5.8.5 Licensees must implement a written cyber security risk policy setting forth the licensee's policies and procedures 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;

(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

CPO-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

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.

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.

CPO-5.8 Cyber Security (continued)

Prevention

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.**

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.**

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

CPO-5.8 Cyber Security (continued)

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

(a) Deployment of anti-virus software and malware programme to detect and isolate malicious code;

(a) Layering systems and systems components;
(b) Build firewalls to reduce weak points through which attacker can gain access to a licensee's network;
(c) Rigorous testing at software development stage to limit the number of vulnerabilities;
(d) Penetration testing of existing systems and networks; and
(e) Use of authority matrix to limit privileged internal or external access rights to systems and data.

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.

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.

Detection

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.

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.

CPO-5.8 Cyber Security (continued)

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 capital market 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.

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.

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.

5.8.19 A licensee must 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. A report submitted to the CBB under this paragraph must be made in accordance with the reporting template as provided in Appendix 1.

Recovery

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.

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.

CPO-5.8 Cyber Security (continued)

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 breach.

Chief Information Security Officer

5.8.23 A licensee's CISO, as referred to in Paragraph CPO-5.8.3(d), is responsible for overseeing and implementing the licensee's cyber security program and enforcing its cyber security policy.

5.8.24 A licensee must submit to the CBB a report, prepared by the CISO and presented to the licensee's board of directors, at least annually, assessing the availability, functionality, and integrity of the licensee's electronic systems, identifying relevant cyber security risks to the licensee, assessing the licensee's cyber security program, and proposing steps for the redress of any inadequacies identified therein.

IT System Audit

5.8.25 The cyber security policy referred to in Rule CPO- 5.8.5 must, at a minimum, include audit functions as set forth below.

(a) Penetration testing: A licensee must conduct penetration testing of its electronic systems, at least annually, and vulnerability assessment of those systems, at least quarterly.

(b) Audit trail: A licensee must maintain audit trail systems that:

(i) track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting;

(ii) protect the integrity of data stored and maintained as part of the audit trail from alteration or tampering;

(iii) protect the integrity of hardware from alteration or tampering, including by limiting electronic and physical access permissions to hardware and maintaining logs of physical access to hardware that allows for event reconstruction;

CPO-5.8 Cyber Security (continued)

(iv) log system events including, at minimum, access and alterations made to the audit trail systems by the systems or by an authorized user, and all system administrator functions performed on the systems; and

(v) maintain records produced as part of the audit trail in accordance with the recordkeeping requirements set forth in this Section.

Application Security

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.

Personnel and Intelligence

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.

6.1 Board of Directors' Responsibility

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.**

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.

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.

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.

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

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.**

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.

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

6.1 Board of Directors' Responsibility (continued)

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.

CPO-6.2 Counterparty Risk

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.

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.

CPO-6.3 Market Risk

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.**

CPO-6.4 Liquidity Risk

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.

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.

CPO-6.5 Operational Risk

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.**

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

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.**

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.

Business Continuity and Disaster Recovery

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

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

(b) identify the supervisory personnel responsible for implementing each aspect of the business continuity and disaster recovery plan;

(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;

CPO-6.5 Operational Risk (continued)

(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.

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

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

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

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

CPO-6.6 Outsourcing

6.6.1 **Licensees must identify all material outsourcing contracts and ensure that the risks associated with such contracts are adequately controlled. In particular, licensees must comply with the specific requirements set out in this Section.**

6.6.2 Outsourcing means an arrangement whereby a third party performs on behalf of a licensee an activity that was previously undertaken by the licensee itself (or in the case of a new activity, one which ordinarily 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.

6.6.3 For purposes of Rule CPO-6.6.1, a contract is 'material' where, if it failed in any way, it would pose significant risks to the on-going operations of a licensee, its reputation and/or the quality of service provided to its clients. For instance, the outsourcing of all or a substantial part of functions such as customer sales and relationship management, settlements and processing, IT and data processing and financial control, would normally be considered "material". Management should carefully consider whether a proposed outsourcing arrangement falls under this Module's definition of "material". If in doubt, management should consult with the CBB.

6.6.4 **For outsourcing services that are not considered material outsourcing arrangements, licensees must submit a written notification to the CBB before committing to the new outsourcing arrangement.**

6.6.5 **Licensees must retain ultimate responsibility for functions or activities that are outsourced. In particular, licensees must ensure that they continue to meet all their regulatory obligations with respect to outsourced activities.**

6.6.6 **Licensees must not contract out their regulatory obligations and must take reasonable care to supervise the discharge of outsourced functions, if any.**

CPO-6.6 Outsourcing (continued)

Supervisory Approach

6.6.7 **Licensees must seek the CBB's prior written approval before committing to a new material outsourcing arrangement.**

6.6.8 **Licensees may not outsource their core business function or activities to third parties.**

6.6.9 **The prior approval request in Rule CPO-6.6.7 must:**

(a) Be made in writing to the licensee's normal supervisory contact; and

(b) Contain sufficient detail to demonstrate that relevant issues raised in this Section have been addressed; and

(c) Be made at least 6 weeks before the licensee intends to commit to the arrangement.

6.6.10 The CBB will review the information provided and provide a definitive response within a reasonable period of time of receiving the request for approval referred to in Rule CPO-6.6.9. The CBB may also contact home or host supervisors to seek their comments – in such cases, the period of time is also subject to the speed of their response.

6.6.11 The CBB's approach to approving requests for outsourcing arrangements will also consider whether the licensee has engaged in considerable outsourcing of its activities, a practice which the CBB does not favour.

6.6.12 **Once an activity has been outsourced, a licensee must continue to monitor the associated risks and the effectiveness of its mitigating controls.**

6.6.13 **Licensees must immediately inform their normal supervisory contact at the CBB of any material problems encountered with an outsourcing provider. The CBB may direct the licensees to make alternative arrangements for the outsourced activity.**

6.6.14 **The CBB requires ongoing access to the outsourced activity, which it may occasionally want to examine, through management meetings or on-site examinations.**

CPO-6.6 Outsourcing (continued)

6.6.15 The CBB reserves the right to require a licensee to terminate or make alternative outsourcing arrangements if, among other reasons, the confidentiality of its client information was, or is likely to be, breached or the ability of the CBB to carry out its supervisory functions in view of the outsourcing arrangement cannot be assured or executed.

6.6.16 In negotiating its contract with a service provider, a licensee should have regard to:

(a) Reporting or notification requirements it may wish to impose on the service provider;
(b) Whether sufficient access will be available to its internal auditors, external auditors and to the CBB;
(c) Information ownership rights, confidentiality agreements and Chinese walls to protect client and other information (including arrangements at the termination of the contract);
(d) The adequacy of any guarantees and indemnities;
(e) The extent to which the service provider must comply with the licensee's policies and procedures (covering, for example, information security)
(f) The extent to which a service provider will provide business continuity for outsourcing operations, and whether exclusive access to its resources is agreed;
(g) The need for continued availability of software following difficulty at a third party supplier; and
(h) The processes for making changes to the outsourcing arrangement (for example, changes in processing volumes, activities and other contractual terms) and the conditions under which the licensee or service provider can choose to change or terminate the outsourcing arrangement, such as where there is:
    (i) A change of ownership or control (including insolvency or receivership) of the service provider;
    (ii) Significant change in the business operations (including subcontracting) of the service provider; or
    (iii) Inadequate provision of services that may lead to the licensee being unable to meet its regulatory obligations.

CPO-6.6 Outsourcing (continued)

6.6.17 Licensees must maintain and regularly review contingency plans to enable them to set up alternative arrangements – with minimum disruption to business – must outsourcing contract be suddenly terminated or the outsourcing provider fails. This may involve the identification of alternative outsourcing providers or the provision of the service in-house. These plans must consider how long the transition would take and what interim arrangements would apply.

6.6.18 A licensee must nominate a relevant approved person within the licensee to handle the responsibility of the day-to-day relationship with the outsourcing provider and to ensure that relevant risks are addressed. The CBB must be informed of the designated individual as part of the request for prior approval required under Rule CPO-6.6.7. Any subsequent replacement of such person must also be notified to the CBB.

6.6.19 All outsourcing arrangements by licensees must be the subject of a legally enforceable contract. Where the outsourcing provider interacts directly with a licensee's clients, the contract must – where relevant – reflect the licensee's own standards regarding customer care. Once an outsourcing agreement has been entered into, licensees must regularly review the suitability of the outsourcing provider and the on-going impact of the agreement on their risk profile and systems and controls framework.

Outsourcing Agreement

6.6.20 The activities to be outsourced and respective contractual liabilities and obligations of the outsourcing provider and licensee must be clearly specified in an outsourcing agreement. This agreement must – amongst other things – address the issues identified below in this Section

CPO-6.6 Outsourcing (continued)

Control Over Outsourced Activities

6.6.21 The Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in outsourced activities. Licensees must therefore ensure they have adequate mechanisms for monitoring the performance of, and managing the relationship with, the outsourcing provider.

6.6.22 Clear reporting and escalation mechanisms must be specified in the agreement.

Client Data Confidentiality

6.6.23 Licensees must ensure that outsourcing agreements comply with all applicable legal requirements regarding client confidentiality.

6.6.24 Licensees must ensure that the outsourcing provider implements adequate safeguards and procedures.

6.6.25 For the purposes of Paragraph CPO-6.6.24, the implementation of adequate safeguards would include the proper segregation of client data from those belonging to other clients of the outsourcing provider. Outsourcing providers should give suitable undertakings that the company and its staff will comply with all applicable confidentiality rules. Licensees should have contractual rights to take action against the service provider in the event of breach of confidentiality.

6.6.26 Licensees must ensure that they retain title under any outsourcing agreements for data, information and records that form part of the prudential records of the licensee.

Access to Information

6.6.27 Outsourcing agreements must ensure that the licensees' internal and external auditors have timely access to any relevant information they may require to fulfil their responsibilities. Such access must allow them to conduct on-site examinations of the outsourcing provider, if required.

CPO-6.6 Outsourcing (continued)

6.6.28 Licensees must also ensure that the CBB inspectors and appointed experts have timely access to any relevant information they may reasonably require to fulfil its responsibilities under the CBB Law. Such access must allow the CBB to conduct on-site examinations of the outsourcing provider, if required.

6.6.29 The outsourcing provider must commit itself, in the outsourcing agreement, to informing the licensee of any developments that may have a material impact on its ability to meet its obligations. These may include, for example, relevant control weaknesses identified by the outsourcing provider's internal or external auditors, and material adverse developments in the financial performance of the outsourcing provider.

Business Continuity

6.6.30 Licensees must ensure that service providers maintain, regularly review and test plans to ensure continuity in the provision of the outsourced service.

6.6.31 Licensees must have an adequate understanding of the outsourcing provider's contingency arrangements, to understand the implications for the licensee's own contingency arrangements.

Termination

6.6.32 Licensees must have a right to terminate the agreement should the outsourcing provider:

(a) Undergo a change of ownership (whether direct or indirect) that poses a potential conflict of interest;
(b) Becomes insolvent; or
(c) Goes into liquidation or administration.

6.6.33 Termination under any other circumstances allowed under the agreement must give licensees a sufficient notice period in which they can effect a smooth transfer of the service to another provider or bring it back in-house.

6.6.34 In the event of termination, for whatever reason, the agreement must provide for the return of all client data – where required by licensees – or destruction of the records.

CPO-6.6 Outsourcing (continued)

Cloud Services

6.6.35 For the purpose of outsourcing of cloud services, licensees must ensure that, at a minimum, the following security measures are in place:

(a) Client information must be encrypted and licensees must ensure that all encryption keys or similar forms of authentication are kept secure within the licensee's control;

(b) A secure audit trail must be maintained for all actions performed at the cloud services outsourcing provider;

(c) A comprehensive change management procedure must be developed to account for future changes to technology with adequate testing of such changes;

(d) The licensee's data must be logically segregated from other entities data at the outsourcing service provider's platform;

(e) The cloud service provider must provide information on measures taken at its platform to ensure adequate information security, data security and confidentiality, including but not limited to forms of protection available against unauthorized access and incident management process in cases of data breach or data loss; and

(f) The right to release client information/data in case of foreign government/court orders must be the sole responsibility of the licensee, subject to the CBB Law.

Intragroup Outsourcing

6.6.36 As with outsourcing to non-group companies, the Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in activities outsourced to group companies.

6.6.37 Licensees must obtain CBB's prior written approval before committing to a material intragroup outsourcing. The request for approval must be made in writing to the licensee's normal supervisory contact at least 6 weeks prior to committing to the outsourcing, and must set out a summary of the proposed outsourcing, its rationale, and an analysis of its associated risks and proposed mitigating controls. All other Rules in this Chapter apply to intragroup outsourcing.

CPO-6.6 Outsourcing (continued)

6.6.38 **Licensees may not outsource their core business activities to their group.**

Internal Audit Outsourcing

6.6.39 **Licensees must not outsource their internal audit function to the same firm that acts as its external auditor.**

6.6.40 Because of the critical importance of an effective internal audit function to a licensee's control framework, all proposals to outsource internal audit operations are to be considered 'material outsourcing agreements'.

6.6.41 **In all circumstances, Board and management of licensees must retain responsibility for ensuring that an adequate internal audit programme is implemented, and will be held accountable in this respect by the CBB.**

CPO-7.1 General Requirements

7.1.1 Notwithstanding the requirements of Module AML – Anti Money Laundering, the crypto asset platform operator must ensure that all of its clients maintain a designated 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 regulatory authority.

7.1.2 Crypto asset platform operators must ensure that any payment of monetary obligations to the client or receipt of monetary entitlements by the client is done through the designated bank account.

7.1.3 Licensees, whether at the commencement of or during a business relationship, must not accept cash from a client, whether for undertaking transactions in accepted crypto-assets or as a payment for services provided by the licensee.

7.1.4 Licensees must not open accounts for pooled funds or receive pooled funds managed by professional intermediaries (such as investment and pension fund managers, stockbrokers and layers or authorized money transferors).

7.1.5 Crypto asset platform operators 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.

7.1.6 Licensees must take measures to ensure that clients do not undertake transactions in accepted crypto-assets as agents (acting on behalf of a third party) as set out in Rule CPO-4.4.4. Therefore, third party verification requirements as specified in Rules AML-1.1.5 to AML-1.1.8 of Module AML are not applicable.

7.1.7 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.

CPO-7.1 General Requirements

7.1.8 Licensees must maintain the following minimum information for all crypto asset transactions involving the payment, receipt, exchange, conversion, purchase, sale, transfer, or transmission of crypto-assets:

(a) the identity and physical addresses of the party or parties to the transaction that are customers of the licensee and, to the extent practicable, any other parties to the transaction;

(b) the amount or value of the transaction, including in what denomination purchased, sold, or transferred;

(c) the method of payment;

(d) the date or dates on which the transaction was initiated and completed; and

(e) a description of the transaction.

CPO-8.1 General Requirements

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-1.1.12(d).**

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 Section 7 at all times.**

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.

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.

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.**

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.**

CPO-8.2 Custodial Arrangements

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.**

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 license 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).

CPO-8.2 Custodial Arrangements

Third Party Crypto-asset Custody Arrangement

8.2.3 For the purposes of Paragraph-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.

8.2.4 In undertaking an appropriate risk assessment of the third party crypto-asset custodian in accordance with Rule-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

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.

CPO-8.2 Custodial Arrangements

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.**

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

8.2.8 **For the purposes of Paragraph CPO-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 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 CPO-4.5.3.**

8.2.9 For the purposes of Paragraph CPO-8.2.2(c), 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.

CPO-8.3 Crypto Wallets

8.3.1 Licensees must put in place necessary rules and regulations for crypto-asset wallets.

8.3.2 For the purposes of Paragraph CPO-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 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 CPO-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.

8.3.3 In addition to the two main crypto-asset wallet types described in Paragraph CPO-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.

CPO-8.3 Crypto Wallets (continued)

8.3.4 Only entities providing the custodial wallets as described in Paragraph CPO-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 CPO-1.1.12(d). With respect to the non-custodial wallets as described in Paragraph CPO-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.

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.

CPO-8.4 Reconciliation, Client Reporting and Record Keeping

Reconciliation

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 all safe custody accepted crypto-assets physically held by the licensee, or its nominee company, 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.

Client Reporting

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.

8.4.3 The statement referred to in Paragraph CPO-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

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.

CPO-8.4 Reconciliation, Client Reporting and Record Keeping (continued)

8.4.5 For the purpose of Paragraph CPO-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.

CPO-9.1 Corporate Governance

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.

CPO-10.1 – Reporting Requirements

Reports Prepared by a Licensee

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).**

10.1.2 **Licensees must submit a Professional Indemnity Insurance Return (Form PIIR) on an annual basis (ref. CPO-4.8.1). Additionally, they must provide, upon request, evidence to the CBB of the coverage in force.**

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 CPO-4.7.5.**

Annual License Fee

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. CPO -1.6.8 and CPO-1.6.9).**

Institutional Information System (IIS)

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.**

10.1.6 Licensees failing to comply with the requirements of Paragraph CPO-10.1.5 or reporting inaccurate information are subject to financial penalties or other enforcement actions.

Reports Prepared by External Auditors

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.**

CPO-10.1 – Reporting Requirements (continued)

Onsite Inspection Reporting

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.

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 ten working days of receipt of such report. Evidentiary documents supporting management's comments must also be included in the response package.

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.

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

10.2 Notification Requirements

General Requirements

10.2.1 **All notifications and approvals required in this Module are to be submitted by licensees in writing.**

10.2.2 In this Module, the term 'in writing' includes electronic communication capable of being reproduced in paper form.

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

10.2.5 **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. CPO-11.3.2).**

10.2 Notification Requirements (continued)

10.2.6 The circumstances that may give rise to any of the events in Paragraph CPO-10.2.6 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.

10.2.8 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

10.2.9 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.

10.2.10 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 CPO-1.7.

Fraud, Errors and other Irregularities

10.2.11 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.**

10.2 Notification Requirements (continued)

Insolvency, Bankruptcy and Winding Up

10.2.12 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

10.2.13 Licensees must notify the CBB of the following:

(a) Removal or resignation of its external auditor; or
(b) Change in audit partner.

Approved Persons

10.2.14 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. CPO-1.7.7).

10.2.15 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.

10.2 Notification Requirements (continued)

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

10.2.17 Overseas crypto-asset exchanger 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.

10.3 Approval Requirements

Change in Name

10.3.1 Licensee must seek prior written approval from the CBB and give reasonable advance notice of a change in:

(a) The licensee's name (which is the registered name of the licensee as a body corporate); or

(b) The licensee's trade name, and that of its subsidiaries located in Bahrain.

10.3.2 The request under Paragraph CPO-10.3.1 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

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.

10.3.4 The request under Paragraph CPO-10.3.4 must include the details of the proposed new address and the date on which the licensee intends to implement the change of address.

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

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.

10.3 Approval Requirements (continued)

Change in Authorised or Issued Capital

10.3.7 As specified in Article 57(a)3 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

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

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.

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.

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

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

10.3.13 Rule CPO-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.

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

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.

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

10.3.18 A licensee must seek prior approval from the CBB for the following:

(a) Outsourcing of their internal audit function (ref. CPO-6.6.40)
(b) Material intra-group outsourcing (ref. CPO-6.6.37);
(c) Outsourcing other material functions (ref. CPO-6.6); or
(d) Other material outsourcing.

10.3 Approval Requirements

Matters Having a Supervisory Impact

10.3.19 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.

10.3.20 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).

10.3.21 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.

10.3.22 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

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 CPO-4.10.3.

External Auditor

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

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).

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).

10.3 Approval Requirements

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. CPO-1.7.7).

Withdrawals

10.3.27 No funds may be withdrawn by shareholders from the licensee without the necessary prior written approval of the CBB.

CPO-11.1 Power to Request Information

11.1.1 Licensees must provide all information that the CBB may reasonably request in order to discharge its regulatory obligations.

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.

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

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.

CPO-11.2 Access to Premises

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.

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.

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.

11.2.4 The cooperation that licensees are expected to procure from such providers is similar to that expected of licensees themselves.

CPO-11.3 Accuracy of Information

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.

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.

11.3.3 If the information in Paragraph CPO-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.

CPO-11.4 Methods of Information Gathering

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 CPO-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 CPO-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.

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.

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;

CPO-11.4 Methods of Information Gathering (continued)

(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)

(f) 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

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

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 CPO-11.4.3:

(a) Its employees; and

(b) Any other members of its group and their employees.

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.

CPO-11.5 The Role of the Appointed Expert

Introduction

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

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.

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.

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.

11.5.5 **Unless the CBB otherwise permits, appointed experts should not be the same firm appointed as external auditor of the licensee.**

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.**

11.5.7 All proposals to appoint appointed experts require approval by an Executive 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.

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

11.5.8 Following the completion of the investigation, the CBB will normally provide feedback on the findings of the investigation to the licensee.

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).

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).

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

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.

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.

11.5.15 Unless otherwise directed by the CBB or unless the circumstances described in Paragraph CPO-11.5.19 apply, the report must be discussed with the Board of directors and/or senior management in advance of it being sent to the CBB.

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

11.5.16 **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.**

11.5.17 **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.**

11.5.18 **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

11.5.19 **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.**

11.5.20 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.

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

11.5.21 If appointed experts decide to communicate directly with the CBB in the circumstances set out in Paragraph CPO-11.5.19, 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

11.5.22 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

11.5.23 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.

This appendix is part of the requirement specified under CPO-5.9.19 (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	