AUTHORISATION MODULE

MODULE:	AU (Authorisation)

Table of Contents

			Date Last Changed
AU-A	**Introduction**		
	AU-A.1	Purpose	01/2022
	AU-A.2	Module History	01/2022
AU-B	**Scope of Application**		
	AU-B.1	The Public	01/2022
	AU-B.2	Licensees and Authorised Persons	07/2010
AU-1	**Authorisation Requirements**		
	AU-1.1	Licensing	XX/2024
	AU-1.2	Approved Persons	01/2021
	AU-1.3	[This Section deleted 07/2007]	07/2007
	AU-1.4	Definition of Regulated Investment Services	01/2022
	AU-1.5	Definition of Financial Instruments	04/2006
AU-2	**Licensing Conditions**		
	AU-2.1	Condition 1: Legal Status	04/2006
	AU-2.2	Condition 2: Mind and Management	01/2021
	AU-2.3	Condition 3: Controllers and Close Links	01/2012
	AU-2.4	Condition 4: Board and Employees	04/2006
	AU-2.5	Condition 5: Financial Resources	07/2010
	AU-2.6	Condition 6: Systems and Controls	04/2006
	AU-2.7	Condition 7: External Auditors	07/2010
	AU-2.8	Condition 8: Other Requirements	04/2006
AU-3	**Approved Persons Conditions**		
	AU-3.1	Condition 1: 'Fit and Proper'	01/2016
	AU-3.2	[This Section was deleted in January 2016]	01/2016
AU-4	**[This Chapter deleted 07/2007]**		
AU-5	**Information Requirements and Processes**		
	AU-5.1	Licensing	10/2019
	AU-5.2	Approved Persons	04/2018
	AU-5.3	[This Section deleted 07/2007]	07/2007
	AU-5.4	Amendment of Authorisation	01/2022
	AU-5.5	Cancellation of Authorisation	07/2015
	AU-5.6	Publication of the Decision to Grant, Cancel or Amend a License	10/2019
AU-6	**License Fees**		
	AU-6.1	License Application Fees	07/2010
	AU-6.2	Annual License Fees	07/2013
Appendix AU-1		Requirements for Regulated Investment Services Involving Crypto Assets	XX/2024

MODULE	AU:	Authorisation
CHAPTER	AU-1:	Authorisation Requirements

AU-1.1 Licensing

AU-1.1.1 **No person may:**

(a) Undertake (or hold themselves out to undertake) regulated investment services, by way of business, within or from the Kingdom of Bahrain unless duly licensed by the CBB;

(b) Hold themselves out to be licensed by the CBB unless they have as a matter of fact been so licensed; or

(c) Market any financial services in the Kingdom of Bahrain unless:

(i) Allowed to do by the terms of a license issued by the CBB;

(ii) The activities come within the terms of an exemption granted by the CBB by way of a Directive; or

(iii) Has obtained the express written permission of the CBB to offer financial services.

AU-1.1.2 For the purposes of Rule AU-1.1.1(a), please refer to Section AU-1.4 for the definition of 'regulated investment services' and 'by way of business. Such 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.

AU-1.1.3 For the purposes of Rule AU-1.1.1(b), persons would be considered in breach of this requirement if they were to trade as, or incorporate a company in Bahrain with a name containing the words (or the equivalents in any language) 'adviser', 'consultant', or 'manager' in combination with "investment", or 'portfolio', without holding the appropriate CBB license or the prior approval of the CBB.

AU-1.1.3A In accordance with Resolution No. (16) for the year 2012 and for the purpose of Subparagraph AU-1.1.1(c), the word 'market' refers to any promotion, offering, announcement, advertising, broadcast or any other means of communication made for the purpose of inducing recipients to purchase or otherwise acquire financial services in return for monetary payment or some other form of valuable consideration.

AU-1.1.3B Persons in breach of Subparagraph AU-1.1.1(c) are considered in breach of Resolution No. (16) for the year 2012 and are subject to penalties under Articles 129 and 161 of the CBB Law (see also Section EN-10.2A).

AU-1.1.4 **Where a person is licensed under Volumes 1 or 2, i.e. as a bank, then a separate license under Volume 4 is not required in order to undertake activities of the kind specified under Section AU-1.4.**

AU-1.1 Licensing (continued)

AU-1.1.5 Persons licensed as banks by the CBB may also undertake the specific activities covered by the definition of regulated investment services (such as trading in financial instruments as principal), since these specific activities also form part of the definition of regulated banking services (or regulated Islamic banking services in the case of Islamic banks). In such cases, banks are not required to hold a separate investment firm license.

AU-1.1.6 **Depending on the type of regulated investment services that a person wishes to undertake, applicants must seek to be licensed either as a Category 1, a Category 2, a Category 3 or a Category 4 investment firm.**

AU-1.1.7 **Persons wishing to be licensed to undertake regulated investment services within or from the Kingdom of Bahrain must apply in writing to the CBB.**

AU-1.1.8 **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 for authorisation of all controllers; and
(c) Application for authorisation of all controlled functions.

AU-1.1.9 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.

AU-1.1.10 Detailed rules and guidance regarding information requirements and processes for licenses can be found in Section AU-5.1. As specified in Paragraph AU-5.1.12, 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.

AU-1.1.11 **All applicants seeking an investment firm license must satisfy the CBB that they meet, by the date of authorisation, the minimum criteria for licensing, as contained in Chapter AU-2. Once licensed, investment firm licensees must maintain these criteria on an on-going basis.**

AU-1.1 Licensing (continued)

Investment Firm License Categories

AU-1.1.12 **For the purposes of Volume 4 (Investment Business), regulated investment services may be undertaken under three categories of investment firms as follows:**

Category 1

AU-1.1.13 **For the purposes of Volume 4 (Investment Business), Category 1 investment firms may undertake (subject to Rule AU-1.1.19) any regulated investment service, as listed below:**

(a) Dealing in financial instruments as principal;
(b) Dealing in financial instruments as agent;
(c) Arranging deals in financial instruments;
(d) Managing financial instruments;
(e) Safeguarding financial instruments (i.e. a custodian);
(f) Advising on financial instruments;
(ff) Arranging Credit and Advising on Credit; and
(g) Operating a collective investment undertaking (i.e. an operator).

AU-1.1.13A **[This Paragraph has been moved to AU-1.1.24].**

AU-1.1.14 [This Paragraph was moved and amended to Paragraph AU-1.4.11A in January 2012].

Category 2

AU-1.1.15 **For the purposes of Volume 4 (Investment Business), Category 2 investment firms may undertake (subject to Rule AU-1.1.19) any regulated investment service (as listed in Rule AU-1.1.13), *except* that of 'dealing in financial instruments as principal'.**

AU-1.1.16 A Category 2 investment firm cannot, therefore, trade in financial instruments for its own account ('dealing in financial instruments as principal'), but it may conduct all other types of regulated investment services, including holding client assets.

AU-1.1 Licensing (continued)

Category 3

AU-1.1.17 **For the purposes of Volume 4 (Investment Business), Category 3 investment firms may undertake (subject to Rules AU-1.1.18 and AU-1.1.19) the following regulated investment services only:**

(a) Arranging deals in financial instruments;
(b) Advising on financial instruments; and
(c) Arranging Credit and Advising on Credit.

AU-1.1.18 **When undertaking either of the regulated investment services listed under Rule AU-1.1.17, Category 3 investment firms:**

(a) Must be independent;
(b) May not hold any client assets;
(c) Must refrain from receiving any fees or commissions from any party other than the client; and
(d) Must not have an 'agency' relationship (tied agent) with an investment provider.

AU-1.1.18A In assessing the independence of a Category 3 investment firm, the CBB will take into account the regulated investment services offered in relation to financial instruments of a related party.

AU-1.1.18B For the purpose of Paragraph AU-1.1.18A, a related party of a Category 3 investment firm includes:

(a) A controller of the Category 3 investment firm as defined in Module GR;
(b) A close link of the Category 3 investment firm as defined in Module GR;
(c) An associate of a controller as defined in Module GR;
(d) The extended family of a controller including a father, mother, father-in-law, mother-in-law, brother, sister, brother-in-law, sister-in-law, or grandparent;
(e) A corporate entity, whether or not licensed or incorporated in Bahrain, where any of the persons identified in Sub-Paragraphs (c) and (d) is a Director or would be considered a controller were the definition of controller set out in Paragraph GR-5.2.1 applied to that corporate entity; and
(f) (This Subparagraph has been deleted).

AU-1.1 Licensing (continued)

Category 4

AU-1.1.18C **For the purposes of Volume 4 (Investment Business), category 4 investment firms are permitted to provide the following regulated investment services to accredited investors:**

a) Operating a collective investment undertaking (CIU); and

b) In respect of venture capital CIUs that the category 4 investment firm operates/manages, act as custodian (i.e. safeguarding financial instruments).

AU-1.1.18D While category 1 investment firms and category 2 investment firms can operate/manage all types of CIUs, targeting retail clients, expert investors and accredited investors, category 4 investment firm license caters to the business models of specialist fund managers who operate/manage CIUs targeted at accredited investors only. Examples of such CIUs are private equity funds, hedge funds, structured funds, real estate funds, venture capital funds and other alternative investment funds. An operator of CIUs who markets or manages a CIU targeted at retail clients or expert investors would not be eligible to obtain a category 4 investment firm license. Category 4 investment firms also act as placement agents of overseas domiciled CIUs they operate/manage.

AU-1.1.18E **Category 4 investment firms must appoint independent custodians to safeguard client assets. However, in accordance with Sub-paragraph AU-1.1.18C(b), category 4 investment firms may be authorised by the CBB to act as custodians of the venture capital CIUs they operate/manage provided they meet the requirements stipulated in Section C4-3.3 of the CBB Rulebook, Volume 4 regarding the safeguarding of client assets and client money. This entails that category 4 investment firms can safeguard the illiquid assets of the venture capital CIUs, but client money must be kept in a client bank account.**

AU-1.1.18F **Category 4 investment firms are only subject to Sections AU-1.1, AU-1.4, AU-1.5 and the provisions of Modules PB, C4, FC and EN. Category 4 investment firms must also comply with CBB Rulebook Volume 7 requirements for authorisation/registration/filing of CIUs to be offered to accredited investors.**

Combining Regulated Investment Services

AU-1.1.19 **Investment firm licensees may combine two or more regulated investment services, providing these fall within the permitted list of services for their investment firm Category, and such combinations are not restricted by Module BC (Business Conduct).**

MODULE	AU:	Authorisation
CHAPTER	AU-1:	Authorisation Requirements

AU-1.1 Licensing (continued)

AU-1.1.20 Module BC (Business Conduct) may restrict licensees from undertaking certain combinations of activities, where such combinations potentially create conflicts of interest that could compromise the interests of customers. See Chapter BC-2.

Suitability

AU-1.1.21 **[This Paragraph was deleted in January 2011].**

AU-1.1.22 [This Paragraph was deleted in January 2011].

AU-1.1.22A **As per Article 48 of the CBB Law, investment firm licensees must seek CBB's prior written approval before undertaking new regulated investment services.**

AU-1.1.22B **Investment firm licensees wishing to undertake the activity of Arranging Credit and Advising on Credit must satisfy the CBB that they have sufficient expertise to undertake this activity and must obtain the CBB's prior written approval for undertaking the same.**

AU-1.1.22C **For purposes of Paragraph AU-1.1.22B, investment firm licensees must ensure that the officer responsible for dealing with the customers for Arranging Credit and Advising on Credit is competent and has demonstrated his competence through appropriate qualifications and experience to carry out such function.**

AU-1.1.22D **Investment firm licensees wishing to undertake the following regulated investment services involving crypto-assets that fall under the definition of financial instruments must seek the CBB's prior approval before undertaking such activity:**
(a) Dealing in financial instruments as agent;
(b) Arranging deals in financial instruments;
(c) Managing financial instruments;
(d) Safeguarding financial instruments (i.e. a custodian);
(e) Advising on financial instruments; and
(f) Operating a collective investment undertaking (i.e. an operator).

Investment firm licensees must not undertake the activity of dealing in crypto-assets as principal.

AU-1.1 Licensing (continued)

AU-1.1.22E **Investment firm licensees offering the regulated investment services referred to in Paragraph AU-1.1.22D must comply with the requirements stipulated in Appendix AU-1, as applicable.**

AU-1.1.22F **Investment firm licensees undertaking the regulated investment service involving safe custody of crypto-assets (custody service), whether through "in house" arrangement or through a "third party", remain responsible for safeguarding, storing, holding or maintaining custody of crypto-assets and must have systems and controls in place to:**

(a) Ensure the proper safeguarding of crypto-assets;

(b) Ensure that such safe custody of crypto-assets is identifiable and secure at all times; and

(c) Ensure protection against the risk of loss, theft or hacking.

AU- 1.1.22G For the purpose of Paragraph AU-1.1.22F, investment firm licensees may implement the following three types of custodial arrangements or any other type of custodial arrangement that is acceptable to the CBB:

(a) The licensee is wholly responsible for custody of client's crypto-assets and provides this service "in-house" through its own crypto-assets wallet solution. Such an arrangement includes scenarios where a licensee provides its own inhouse proprietary wallet for clients to store any crypto-assets bought through that licensee or transferred into the wallet from other sources.

(b) The licensee is wholly responsible for the custody of client's crypto-assets but outsources this service to a third party crypto-asset custodian. Such an arrangement includes the scenario where a licensee uses a third-party service provider to hold all its clients' crypto-assets (e.g., all or part of the clients' private keys).

(c) The licensee wholly allows clients to "self-custodise" their crypto-assets. Such an arrangement includes scenarios where licensees require clients to self-custodise their crypto-assets. Such licensees only provide the platform for clients to buy and sell crypto-assets. Clients are required to source and use their own third party crypto-asset custodians (which the licensee have no control over or responsibility for). This arrangement also includes the scenario where licensees provide an in-house wallet service for clients, but also allow clients to transfer their crypto-assets out of this wallet to another wallet from a third-party wallet provider chosen by the client (and which the licensee does not control).

AU-1.1 Licensing (continued)

AU-1.1.22H Where investment firm licensees provide a third-party crypto-asset custodian to a client it must undertake an appropriate risk assessment of that crypto-asset custodian. Licensees must also retain ultimate responsibility for safe custody of crypto-assets held on behalf of clients and ensure that they continue to meet all their regulatory obligations with respect to crypto-asset custody service and outsourced activities.

AU-1.1.22I Investment firm licensees offering the regulated investment services referred to in Paragraph AU-1.1.22D must provide a report from an independent third-party expert that they have established adequate policies, procedures, systems and controls to manage the associated risks and undertake such activities in compliance with the requirements of Chapter FC-11 and Appendix AU-1. In addition, licensees must satisfy the CBB that they have sufficient competence and expertise to undertake the activities.

AU-1.1.22J For purpose of Paragraph AU-1.1.22D, investment firm licensees must submit a board resolution to undertake the activity together with the following information:

(a) Description of the services/products;
(b) Changes to organisation structure and framework (if any);
(c) Experience of resources responsible for such services and their details; and
(d) Enhancements to its risk management framework to capture, monitor, measure, control and report risks arising from the activity.

Conventional and Islamic Investment Firms

AU-1.1.23 Investment firm licensees may deal in both conventional and Islamic financial instruments. Only those investment firm licensees whose operations are fully Shari'a compliant, however, may hold themselves out to be an Islamic investment firm.

AU-1.1.24 Where licensees are undertaking regulated activities in accordance with Shari'a, all transactions and contracts concluded by investment firm licensees must comply with Shari'a standards issued by the Accounting and Auditing Organisation for Islamic Financial Institutions (AAOIFI). The validity of the contract or transaction is not impacted, if at a later date, the relevant AAOIFI Shari'a standard are amended.

AU-1.1 Licensing (continued)

AU-1.1.24A **In accordance with Paragraph HC-9.2.1, Category 1 and 2 Islamic investment firms must maintain a Shari'a Supervisory Board, comprised of at least 3 Shari'a board members, to verify that their operations are Shari'a compliant.**

AU-1.1.24B **Category 3 and Category 4 Islamic investment firms must appoint a minimum of one Shari'a advisor or scholar to verify that their operations are Shari'a compliant.**

AU-1.1.25 **Investment firm licensees (whether conventional or Islamic) may not accept Shari'a money placements or deposits. They may not enter into Shari'a financing contracts (except where it is an incidental part of assisting a client to buy, sell, subscribe for or underwrite a financial instrument). Finally, they may not offer Shari'a Profit Sharing Investment Accounts (whether restricted or unrestricted).**

AU-1.1.26 Shari'a money placements or deposits include money taken under *q'ard* or *al-wadia* contracts. Shari'a financing contracts include contracts such as *murabaha*, *bay muajjal*, *bay islam*, *ijara wa iktina* and *istisna'a*. Profit sharing investment accounts include those accounts undertaken under *mudaraba* and *musharaka* contracts.

AU-1.1.27 The transactions prohibited under Rule AU-1.1.25 may only be undertaken by bank licensees.

Appendix AU-1: Requirements for Regulated Investment Services Involving Crypto Assets

Introducing/Offering Crypto-assets to Clients

1. **Licensees must establish a policy which lays down the internal procedure and risk assessment that a licensee must undertake prior to introducing a crypto-asset for trading by its clients. The policy must be approved by the board and reviewed periodically.**

2. **Prior to introducing a crypto-asset, a licensee must notify the CBB of its intent to introduce the crypto-asset, provide the findings of the risk assessment undertaken in accordance with Point 8 below along with the board resolution approving the crypto-asset.**

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

4. **Licensees must have necessary blockchain monitoring capability (e.g. via monitoring systems, internal monitoring control etc.) in place before introducing the crypto-asset on its platform.**

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

6. **Licensees must ensure that:**
   - **(a) any actual or potential conflicts of interest in connection with the review and decision-making process have been assessed and effectively addressed, whether such actual or potential conflicts of interest are related to the licensee's board members, shareholders employees, their families, or any other party; and**
   - **(b) records are maintained of the licensee's due diligence of each crypto-asset. This includes the final approval for introducing a crypto-asset, the documents the board of directors reviewed including an assessment of all associated material risks in connection with each crypto-asset approval or disapproval, such as reviews and sign-offs by various departments of the licensee, such as the legal, compliance, cybersecurity, and operations department etc.**

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

Risk Assessment

8. Licensees must establish criteria and undertake a comprehensive risk assessment of the crypto-assets that it intends to offer on its platform. The risks to be assessed must include, but are not limited to, the following:
   (a) Licensees must conduct a thorough due diligence process to ensure that the crypto-asset is created or issued for lawful and legitimate purposes, and not for evading compliance with applicable laws and regulations (e.g., by facilitating money laundering or other illegal activities) and that the process is subject to a strong governance and control framework. Licensees must consider the following factors while undertaking the due diligence:
      (i) The technological experience, track record and reputation of the issuer and its development team;
      (ii) The availability of a reliable multi-signature hardware wallet solution;
      (iii) The protocol and the underlying infrastructure, including whether it is: (1) a separate blockchain with a new architecture system and network or it leverages an existing blockchain for synergies and network effects, (2) scalable, (3) new and/or innovative or (4) the crypto-asset has an innovative use or application;
      (iv) The relevant consensus protocol;
      (v) Developments in markets in which the issuer operates;
      (vi) The geographic distribution of the crypto-asset and the relevant trading pairs, if any;
      (vii) Whether the crypto-asset has any in-built anonymization functions;
      (viii) Crypto-asset exchanges on which the crypto-asset is traded.

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

(h) Risks relating to potential non-compliance with the requirements of the licensee's condition and regulatory obligations as a result of the offering of new crypto-asset;
(i) Legal risks associated with the new crypto-asset, including any pending or potential civil, regulatory, criminal, or enforcement action relating to the issuance, distribution, or use of the new crypto-asset; and
(j) Type of distributed ledger: whether there are issues relating to the security and/or usability of a distributed ledger technology used for the purposes of the crypto-asset; whether the crypto-asset leverages an existing distributed ledger for network and other synergies; whether this is a new distributed ledger that has been demonstrably stress tested.

Periodic Monitoring

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

Disclosure

10. Licensees must make adequate disclosures, which are easily accessible and prominently visible to clients, for each crypto-asset, containing at a minimum, the following information:
    (a) Details about the crypto-asset: the type of crypto-asset (payment token, asset token, utility token, stablecoin etc.), its function and details about the asset(s) where a crypto-asset is backed by asset(s);
    (b) The risks related to the specific crypto-asset such as, but not limited to, price volatility and cyber-security; and
    (c) Any other information that would assist clients to make an informed investment decision.

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

Crypto-asset Custody

12. A licensee intending to offer crypto-asset custody service must provide to the CBB, for prior written approval, details of custodial arrangement put in place to safeguard, store, hold or maintain custody of crypto-assets.

13. To the extent a licensee stores, holds, or maintains custody or control of crypto-assets on behalf of a client, such licensee must hold crypto-assets of the same type and amount as that which is owed or obligated to such other client.

14. A licensee is prohibited from selling, transferring, assigning, lending, hypothecating, pledging, or otherwise using or encumbering crypto-assets stored, held, or maintained by, or under the custody or control of, such licensee on behalf of a client except for the sale, transfer, or assignment of such crypto-asset at the direction of the client.

15. A licensee that undertakes crypto-asset custody service through 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.

16. A licensee that maintains custody or control of crypto-assets on behalf of a client must store, at a minimum, 90% of client's crypto-assets in cold wallets to minimise exposure to losses arising from a compromise or hacking. The requirement to hold 90% of client's crypto-assets in cold wallet is to be calculated separately for each crypto-asset that is offered on the licensee's platform and not at aggregate level.

17. A licensee must have a documented policy detailing the mechanism for the transfer of crypto-assets between hot, cold and other storage. The scope of authority of each function designated to perform any non-automated processes in such transfers must be clearly specified in the policy document.

18. A licensee that maintains custody or control of crypto-assets must not, at any time, permit arrangements whereby just a party or signatory is able to completely authorise the movement, transfer or withdrawal of crypto-assets held under custody on behalf of clients. In particular, licensees must not have custody arrangements whereby only a sole person can fully access the private key or keys for the crypto assets held under custody by the licensee.

19. Licensees that maintain custody or control of crypto-assets are required to have policies and procedures in place that clearly describe the process that will be adopted in the event that the licensee comes to know or suspects that the crypto-assets it is holding under custody on behalf for clients have been compromised, such as in the event of a hacking attack, theft or fraud. Such policies and procedures must detail the specific steps the licensee will take to protect client's crypto-assets in the event of such incidents. Licensees must also have the ability to immediately halt all further transactions with regard to the crypto-assets.

20. Licensees must have written procedures for dealing with events such as forks (hard, soft or temporary forks) or air drops from an operational and technical point of view.

21. Where a licensee supports a new protocol, it must ensure that changes in the underlying protocol of a crypto-asset that result in a fork are managed and tested proactively. This includes temporary forks which should be managed for reverse compatibility for as long as required. Where a licensee supports a new protocol, a licensee must ensure that their clients are able to deposit and withdraw crypto-assets in and out of the wallet as and when requested before and after a fork (except during go-live). Clients must be notified well in advance of any periods of time when deposits and withdrawals are not feasible.

22. Where the underlying protocol of a crypto-asset is changed, and the older version of the crypto-asset is no longer compatible with the new version and/or there is an entirely new and separate version of the crypto asset (hard fork), licensees must ensure that client balances on the old version are reconciled with the new version of the crypto-asset. This includes availability of reverse compatibility for as long as required. Licensees maintain transparent lines of communication with their clients on how they are managing clients crypto-asset holdings in such a scenario.

23. In the case of a hard fork, a licensee, where it supports a new protocol, must proactively manage any discrepancy between the balances recorded on the previous version versus the new version by engaging with the entity which is responsible for updating and supporting the underlying protocol of the relevant crypto-asset. Additionally, licensees must ensure that, where they seek to offer services in relation to the crypto-asset associated with the new version of the underlying protocol, this new crypto-asset meets the requirements for a crypto-asset and that they notify the CBB well in advance of offering the new crypto-asset as part of its activities.

24. In compliance with Paragraph AU-1.1.22H, when undertaking an appropriate risk assessment of the third party crypto-asset custodian, licensees should take into account the following:

(a) The expertise and market reputation of the third party crypto-asset custodian, and once a crypto-asset has been lodged by the licensee with the third party crypto-asset custodian, the crypto-asset custodian's performance of its services to the licensee;
(b) The arrangements, including cyber security measures, for holding and safeguarding crypto-assets;
(c) An appropriate legal opinion as to the protection of crypto-assets in the event of insolvency of the custodian;
(d) Whether the third party crypto-asset custodian is regulated and by whom;
(e) The capital or financial resources of the third party crypto-asset custodian;
(f) The credit rating of the third party crypto-asset custodian; and
(g) Any other activities undertaken by the third party crypto-asset custodian and, if relevant, any affiliated company.

25. Licensees should consider, at the minimum, the following two types of crypto-asset wallets:

(a) Custodial Wallet: the custodial wallet provider holds crypto-assets (e.g., the private keys) as an agent on behalf of clients, and has at least some control over these crypto-assets. Licensees that hold crypto-assets on behalf of their clients should generally offer custodial wallets and may even offer multi-signature wallets. Clients using custodial wallets do not necessarily have full and sole control over their crypto-assets. In addition, there is a risk that should the custodial wallet provider cease operations or get hacked, clients may lose their crypto-assets; and

(b) Non-Custodial (Self-Custody) Wallets: the non-custodial wallet provider, typically a third-party hardware add/or software company, offers the means for each client to hold their crypto-assets (and fully control private keys) themselves. The non-custodial wallet provider does not control client's crypto-assets – it is the client that has sole and full control over their crypto-assets. Hardware wallets, mobile wallets, desktop wallets and paper wallets are generally examples of non-custodial wallets. Clients using non-custodial wallets have full control of and sole responsibility for their crypto-assets, and the non-custodial wallet provider does not have the ability to effect unilateral transfers of clients' crypto-assets without clients' authorisation.

In addition to the two main crypto-asset wallet types described 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.

Only entities providing the custodial wallets as described in above are considered to be carrying out the regulated activity of safeguarding, storing, holding, maintaining custody of or arranging custody on behalf of clients for crypto-assets. With respect to the non-custodial wallets as described above, the wallet provider is merely providing the technology; it is the wallet user himself who has full control of and responsibility for his crypto-assets.

26. Licensees must assess the risks posed to each storage method in view of the new developments in security threats, technology and market conditions and must implement appropriate storage solutions to ensure the secure storage of crypto-assets held on behalf of clients. Wallet storage technology and any upgrades should be tested comprehensively before deployment to ensure reliability. A licensee must implement and must ensure that its third-party crypto-asset custodian implements, measures to deal with any compromise or suspected compromise of all or part of any seed or private key without undue delay, including the transfer of all client crypto-assets to a new storage location as appropriate.

27. Licensees must have, or where the licensee uses the service of a third party crypto-asset custodian must ensure that the third party crypto-asset custodian has, adequate processes in place for handling deposit and withdrawal requests for crypto-asset to guard against loss arising from theft, fraud and other dishonest acts, professional misconduct or omissions. In this regard, a licensee must:
    (a) continuously monitor major developments (such as technological changes or the evolution of security threats) relevant to all crypto-assets included for trading. There must be clear processes in place to evaluate the potential impact and risks of these developments, as well as for handling fraud attempts specific to distributed ledger technology (such as 51% attacks), and these processes should be proactively executed;
    (b) ensure that client IP addresses as well as wallet addresses used for deposit and withdrawal are whitelisted, using appropriate confirmation methods;
    (c) have clear processes in place to minimise the risks involved with handling deposits and withdrawals, including whether deposits and withdrawals are performed using hot or cold storage, whether withdrawals are processed on a real-time basis or only at certain cut-off times, and whether the withdrawal process is automatic or involves manual authorisation;
    (d) ensure that any decision to suspend the withdrawal of crypto-assets is made on a transparent and fair basis, and is communicated without delay to all its clients; and
    (e) ensure that the above processes include safeguards against fraudulent requests or requests made under duress as well as controls to prevent one or more officers or employees from transferring assets to wallet addresses other than the client's designated wallet address.

28. A licensee must at least every calendar month:
    (a) reconcile all crypto-assets held by the licensee, or its third-party custodian, and reconcile the result to the records of the licensee; and
    (b) reconcile individual client balances with the licensee's records of crypto-assets balances held in client accounts; and
    (c) where the licensee discovers discrepancies after carrying out the above reconciliations, it must maintain a record of such discrepancies and the measures taken to remedy such discrepancies.

Key Management and Wallet Storage

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

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

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

32. 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.

33. Crypto assets that do not need to be immediately available must be held offline, in a 'cold wallet'.

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

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

36. 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.

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

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.

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

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

    (a) The generated seed and private key must be sufficiently resistant to speculation or collusion. The seed and private key must be generated in accordance with applicable international security standards and industry best practices, so as to ensure that the seeds (where Hierarchical Deterministic Wallets, or similar processes, are used) or private keys (if seed are not used) are generated in a non-deterministic manner which ensures randomness and thus are not reproducible. Where practicable, seed and private key must be generated offline and kept in a secure environment, such as a Hardware Security Module (HSM), with appropriate certification for the lifetime of the seeds or private keys;
    (b) Detailed specifications for how access to cryptographic devices or applications is to be authorised, covering key generation, distribution, use and storage, as well as the immediate revocation of a signatory's access as required;
    (c) Access to seed and private key relating to crypto-assets is tightly restricted among approved persons, no single approved person has possession of information on the entirety of the seed, private key or backup passphrases, and controls are implemented to mitigate the risk of collusion among authorised personnel; and
    (d) Distributed backups of seed or private key is kept so as to mitigate any single point of failure. The backups need to be distributed in a manner such that an event affecting the primary location of the seed or private key does not affect the backups. The backups should be stored in a protected form on external media (preferably HSM with appropriate certification). Distributed backups should be stored in a manner that ensures seed and private key cannot be re-generated based solely on the backups stored in the same physical location. Access control to the backups needs to be as stringent as access control to the original seed and private key.

39. Licensees must establish, maintain and implement a private key storage policy to ensure effective and prudent safekeeping of the seed and private key at all times. In particular, such policy must address:
    (a) the keyman risk associated with the storage of seed and private key is appropriately addressed;
    (b) the seed and private key can be retrieved at a short notice without excessive reliance on one or more individuals who may be unavailable due to death, disability or other unforeseen circumstances; and
    (c) where a licensee maintains a physical copy of the seed and private key, the physical copies of seed and private key must be maintained in Bahrain in a secure and indestructible manner and the same can be used to access the wallets if need arises.

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

Transaction with Counterparties

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

(a) the use of proxies, any unverifiable or high-risk IP geographical locations, disposable email addresses or mobile numbers, or frequently changing the devices used to conduct transactions; and
(b) transactions involving tainted wallet addresses such as "darknet" marketplace transactions and those involving tumblers.
(c) where an applicant's IP address is masked a licensee must take reasonable steps to unmask the IP address or decline to provide services to that applicant.

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

(a) identify and prohibit transactions with wallet addresses or their equivalent which are compromised or tainted; and
(b) employ technology solutions which enable the tracking of crypto-assets through multiple transactions to more accurately identify the source and destination of these crypto-assets.

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

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

Disclosure to Clients

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

(a) a crypto-asset is not a legal tender and is not backed by the government;
(b) legislative and regulatory changes or actions at national level or international level may adversely affect the use, transfer, exchange, and value of crypto-assets;
(c) transactions in crypto-assets may be irreversible, and, accordingly, losses due to fraudulent or accidental transactions may not be recoverable;
(d) some crypto-asset transactions may be deemed to be made when recorded on a public ledger, which is not necessarily the date or time that the client initiates the transaction;

(e) the value of crypto-assets may be derived from the continued willingness of market participants to exchange fiat currency for crypto-asset, which may result in the potential for permanent and total loss of value of a particular crypto-asset should the market for that crypto-asset disappear;
(f) the volatility and unpredictability of the price of crypto-assets relative to fiat currency may result in significant loss over a short period of time;
(g) cybersecurity risks associated with crypto-assets including the risk of partial or full loss of crypto-assets in the event of a cyber-attack, and measures that have been put in place to mitigate the cyber security risks;
(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;
(i) any investor protection mechanism;
(j) the rights and entitlements of a client when events such as, but not limited to, forks and airdrops occur;
(k) how they execute and route client's order and source liquidity (e.g. whether they pass or route orders to an exchange to execute). Where the licensee routes client orders to one or more crypto-asset exchanges for execution, it must disclose details of all the crypto-asset exchanges; and
(l) how it determines the prices of the crypto-assets it quotes to clients.

Prevention of Fraud

43. Licensees must take reasonable steps to detect and prevent fraud, including by establishing and maintaining a written anti-fraud policy. The anti-fraud policy must, at a minimum, include:
(a) the identification and assessment of fraud-related risk areas;
(b) procedures and controls to protect against identified risks;
(c) allocation of responsibility for monitoring risks and establish real-time/near real-time fraud risk monitoring and surveillance system; and
(d) procedures for the periodic evaluation and revision of the anti-fraud procedures, controls, and monitoring mechanisms.

44. 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.

(c) Origin and destination of crypto-assets: Systems and controls to mitigate the risk of misuse of crypto-assets, setting out how:
  (i) the origin of crypto-asset is determined, in case of an incoming transaction; and
  (ii) the destination of crypto-asset is determined, in case of an outgoing transaction.

Professional Indemnity Insurance

45. Licensees must ensure that professional indemnity insurance, inter alia:

(a) Covers any legal liability in consequence of any negligent act, error or omission in the conduct of the licensee's business by the licensee or any person employed by it or otherwise acting for it, including consultants under a contract for service with the licensee;
(b) Covers legal defence costs which may arise in consequence of any negligent act, error or omission in the conduct of the licensee's business by the licensee or any person employed by it or otherwise acting for it, including consultants under a contract for service with the licensee;
(c) Covers any legal liability in consequence of any dishonest, fraudulent, criminal or malicious act, error or omission of any person at any time employed by the licensee, or otherwise acting for it, including consultants under a contract for service with the licensee; and
(d) Covers loss of and damage to documents and records belonging to the licensee or which are in the care, custody or control of the licensee or for which the licensee is responsible; including also liability and costs and expenses incurred in replacing, restoring or reconstructing the documents or records; including also consequential loss resulting from the loss or damage to the documents or records.