Stablecoin Issuance and Offering Module

MODULE:	SIO (Stablecoin Issuance and Offering)

Table of Contents

MODULE:	SIO (Stablecoin Issuance and Offering)

Table of Contents

MODULE:	SIO (Stablecoin Issuance and Offering)

Table of Contents

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-A	Introduction

SIO-A.1 Purpose

Executive Summary

SIO-A.1.1 Module SIO formulates the regulatory framework of the Central Bank of Bahrain ('CBB') to govern the issuance and offering of stablecoins in/from the Kingdom of Bahrain. These regulations are issued pursuant to the authority of the CBB under Article 37 to establish and enforce rules, while meeting the specific requirements of Part 4 of the Central Bank of Bahrain and Financial Institutions Law of 2006 ("CBB Law"). The requirements pertaining to licensing, issuance and offering of stablecoins to public are outlined in this Module. Licensed stablecoin issuers are also subject to other relevant Modules of the CBB Rulebook Volume 6.

SIO-A.1.2 The requirements of this Module must be read together with other relevant law, rules, regulations including the AML/CFT Law and the following Modules of CBB Rulebook Volume 6:

(a) Anti-Money Laundering and Combating Financial Crime Module;

(b) Fit and Proper Requirements Module (currently under consultation)

(c) High Level Control Module of Volume 6.

Legal Basis

SIO-A.1.3 This Module contains the CBB's Directive (as amended from time-to-time) relating to issuance and offering of stablecoins and is issued under the powers available to the CBB under Article 38 of the CBB Law. Licensed stablecoin issuers must also comply with the relevant Modules of the Rulebook Volume 6.

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

SIO-A.2 Module History

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

Module Ref.	Change Date	Description of Changes

Effective Date

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

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-1	Scope of Application

SIO 1.1 Undertaking Regulated Activity in Stablecoins

SIO-1.1.1 **This Module sets out the requirements for stablecoin issuers undertaking regulated stablecoin offering service. Regulated stablecoin offering service includes the issuance and offering of, controlling the total supply of, minting and burning of stablecoin as well as services incidental to issuance and offering of stablecoin such as managing and safeguarding the reserve assets and custody of stablecoins.**

SIO-1.1.2 **Pursuant to CBB Regulation No (1) of 2007 with respect to services regulated by the CBB (as amended), issuance and offering of stablecoins is a regulated activity and a person must not undertake such regulated activities in or from the Kingdom of Bahrain unless the Central Bank of Bahrain's written approval is granted.**

SIO-1.1.3 **Stablecoin issuers must satisfy the conditions and requirements detailed in this Module for:**
(a) The types of stablecoins that can be issued; and
(b) The requirements pertaining to stablecoin issuer's eligibility and obligations.

SIO-1.1.4 **No person shall undertake the regulated stablecoin offering service within or from the Kingdom of Bahrain, without obtaining the necessary license from the CBB.**

SIO-1.1.5 The regulated 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) Solicits clients within the Kingdom of Bahrain.

SIO-1.1.6 To assist with the interpretation of the requirements of this Module and their application, stablecoin issuer and/or their appointed functionaries should initiate discussion with the CBB and seek necessary clarification. Any action or conduct which departs from the requirements stipulated in this Module or other applicable Modules shall be taken into account by the CBB for the purpose of determining compliance with the regulatory framework.

SIO-1.2 Type of Stablecoins Permitted for Offering

SIO-1.2.1 **Stablecoin issuers are permitted to issue fully backed single currency stablecoin backed by one of the following fiat currencies:**
(a) Bahraini Dinar (BHD);
(b) United States Dollar (USD); and
(c) Any other fiat currency acceptable to the CBB and in respect of which a prior CBB approval has been obtained

SIO-1.2.2 **For the purpose of Paragraph SIO-1.2.1, an approved stablecoin must be fully backed (1:1) by the same fiat currency it purports to be tokenising.**

SIO-1.2.3 With regards to Paragraph SIO-1.2.1(c) above, the CBB while determining the suitability of stablecoins backed in any other fiat currency (other than Bahraini Dinar and US Dollar), will take into consideration various factors including but not limited to the stabilisation mechanism as well as the availability of high quality and highly liquid with minimal market, credit and concentration risk reserve assets in those currencies.

SIO-1.2.4 In order to distinguish stablecoins approved by the CBB for offering pursuant to the requirement of this Module from other types of stablecoins, the stablecoins approved by the CBB shall be referred to as approved stablecoins.

CBB's Right of Refusal or Restrictions on Stablecoin Offering

SIO-1.2.5 The CBB may reject an application for issuance of stablecoin if it determines that the issuance thereof might cause damage, dilute or be contrary to the interests of national economy, the holders of the stablecoin or public investors in general. The CBB may also refuse to grant its approval, postpone granting such approval, or impose additional terms and conditions on the issuance of stablecoins, if the CBB deems that the market condition or circumstances justifies such action.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-2	Licensing

SIO-2.1 Application for License

SIO-2.1.1 **Applicants for a stablecoin issuer 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 Paragraph SIO-2.1.4, unless otherwise directed by the CBB.**

SIO-2.1.2 **Applicants seeking a stablecoin issuer 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.**

SIO-2.1.3 References to applicant mean the potential 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.

SIO-2.1.4 **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 provided for in Paragraph SIO-2.5.2) in the proposed licensee;

(c) A comprehensive business plan for the application, addressing the matters described in Paragraph SIO-2.1.6;

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

(e) A certified copy of a Board resolution of the applicant, confirming its decision to seek a CBB stablecoin issuer license;

(f) In the case of applicants that are part of a group, a letter of no 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;

(g) 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;

(h) In the case of applicants not falling under (g) above, copies of the audited financial statements of the applicant's substantial

SIO-2.2 Application for License (Continued)

shareholder (where they are a legal person), for the three years immediately prior to the date of application;

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

(j) A draft stablecoin whitepaper with all the information pertaining to the stablecoin as stipulated in Chapter 7; and

(k) A description of the system and procedure in place to safeguard the integrity and confidentiality of data;

(l) Details of their proposed external auditor to the CBB as part of their license application.

SIO-2.1.5 The CBB, in its absolute discretion, may ask for a letter of guarantee from the applicant's controlling or major shareholders on a case-by-case basis as it deems appropriate/necessary as part of the required documents to be submitted pursuant to Paragraph SIO- 2.1.4 above.

SIO-2.1.6 **The business plan submitted in support of an application must include:**

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

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

(c) Particulars of supervisory authority together with contact information for the businesses in jurisdictions that are subject to regulation;

(d) The reasons for applying for a license, including the applicant's analysis of the feasibility and market viability, market size and strategy and market objectives;

(e) Description of geographic segments in which the applicant will operate from Bahrain;

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

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

(h) Detailed business process flows from end to end for each significant service/product offering;

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

(j) An opening balance sheet for the applicant, together with a three year financial projection (i.e. balance sheet, income statement, cash flows statement and statement of change in equity), with all assumptions clearly outlined;

SIO-2.1 Application for License (Continued)

demonstrating that the applicant will be able to meet applicable capital adequacy requirements;

(k) Details of banking arrangements, reserve asset management arrangement and approved stablecoin custody arrangement;

(l) A copy of business continuity plan; and

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

SIO-2.1.7 The applicant's memorandum and articles of association must explicitly provide for it to undertake the activities proposed in the license application and must preclude the applicant from undertaking other regulated services, or commercial activities, unless these arise out of its regulated stablecoin issuance services or are incidental to those.

SIO-2.1.8 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.

SIO-2.1.9 Any material changes or proposed changes to the information provided to the CBB in support of a licensing application that occurs prior to licensing must be reported to the CBB.

SIO-2.1.10 Failure to inform the CBB of the changes specified in Paragraph SIO-2.1.9 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 SIO-3.1.1 (i)

Licensing Process and Timelines

SIO-2.1.11 Articles 44 to 47 of the CBB Law govern the licensing process which stipulate that the CBB will issue its decision within 60 calendar days of an application being deemed complete (i.e. containing all required information and documents). By law, the 60 days' time limit only applies once the application is complete and all required information (which may include any clarifications requested by the CBB) and documents have been provided. This means that all the information specified in Paragraph SIO-2.1.4 should be provided, before the CBB may issue a license.

SIO-2.1.12 Potential applicants are encouraged to contact the CBB at an early stage to discuss their plans, for guidance on the CBB's license 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.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-2	Licensing

SIO-2.1 Application for License (Continued)

SIO-2.1.13 Potential applicants should initiate pre-application meetings in writing, setting out a short summary of their proposed business and any issues or questions that they may have already identified, once they have a clear business proposition in mind and have undertaken their preliminary research. The CBB can then guide the applicant on the specific areas in the Rulebook that will apply to them and the relevant requirements that they must address in their application.

SIO-2.1.14 An applicant must not hold himself out as having been licensed by the CBB, prior to the issuance of the CBB's Resolution on granting the license. Failure to do so may constitute grounds for refusing an application and result in a contravention of Article 42 of the CBB Law (which carries a maximum penalty of BD 1 million).

Granting or Refusal of License

SIO-2.1.15 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.

SIO-2.1.16 The CBB may reject an application for a license if in its opinion:

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

SIO-2.1.17 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.

SIO-2.1.18 Before the final approval is granted to an applicant, a confirmation from a licensed 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.

SIO-2.1 Application for License (Continued)

Commencement of Operations

SIO-2.1.19 **Prior to commencement of operation a stablecoin issuer 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 stablecoin issuer;

(b) The stablecoin issuer's contact details including telephone and fax number, e-mail address and website;

(c) A copy of the auditor's acceptance to act as auditor for the applicant;

(d) A copy of the applicant's notarized memorandum and articles of association, addressing the matters described in Paragraph SIO-2.1.9;

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

(f) A written confirmation from the bank, financial institution and custodian, addressed to the CBB providing details about the banking arrangements for subscription money, reserve asset management arrangement and custody arrangement that has been made by the stablecoin issuer;

(g) Where the stablecoin issuer has entered into an agreement with a third party for custody arrangement, a copy of the written agreement between the stablecoin issuer and the third party.

SIO-2.1.20 **Licensed stablecoin issuers must commence their commercial operations within 6 months of being granted a license by the CBB, failing which the CBB may cancel the license, in accordance with the provisions of the CBB Law.**

SIO-2.1.21 In addition, the CBB may vary existing requirements or impose additional restrictions or requirements, beyond those already specified for stablecoin issuers, to address specific risks.

SIO-2.2 Voluntary Surrender, Cancellation or Amendment of License

Voluntary Surrender of a License

SIO-2.2.1 **In accordance with Article 50 of the CBB Law, a stablecoin issuer intending to cease carrying out all the approved regulated stablecoin offering services, must obtain the CBB's written approval, before ceasing regulated stablecoin offering services. 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.**

SIO-2.2.2 **Stablecoin issuers must satisfy the CBB that their clients' interests are to be safeguarded during and after the proposed cancellation.**

SIO-2.2.3 The CBB will approve a request for cancellation of license by a stablecoin issuer where there are no outstanding regulatory concerns and client interests would not be prejudiced. A voluntary surrender will only be allowed to take effect once the stablecoin issuer, in the opinion of the CBB, has discharged all its regulatory obligations towards clients.

Cancellation of a License by the CBB

SIO-2.2.4 Pursuant to Article 48 (c) of the CBB Law, the CBB may cancel a license, for instance if a stablecoin issuer fails to satisfy any of its existing license conditions or in order to protect the legitimate interests of clients or creditors of the licensee. The CBB generally views the cancellation of a license as appropriate only in the most serious of circumstances, and generally tries to address supervisory concerns through other means beforehand.

SIO-2.2.6 The procedures for cancellation of a license are contained in Articles 48 and 49 of the CBB Law.

SIO-2.2.6 The CBB will only effect the cancellation once a stablecoin issuer 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 stablecoin issuer so that no new regulated stablecoin issuance may be undertaken whilst the licensee discharges its obligations to its clients.

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

SIO-2.2.7 **Stablecoin issuers wishing to vary the scope of the regulated stablecoin offering services under their existing license, whether by adding or ceasing some services, must obtain CBB's prior written approval.**

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-2	Licensing

SIO-2.3 Publication of the Decision to Grant, Cancel or Amend a License

SIO-2.3.1 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.

SIO-2.3.2 For the purposes of Paragraph SIO-2.3.1, the cost of publication must be borne by the stablecoin issuer.

SIO-2.3.3 The CBB may also publish its decision on such cancellation or amendment using any other means it considers appropriate, including electronic means.

SIO-2.4 Annual License Fees

SIO-2.4.1 **Licensed stablecoin issuers must pay a variable annual license fee to the CBB amounting to 0.25% of aggregate operating expenses of the preceding year subject to a minimum fee of BD 5,000 and maximum fee of BD 12,000, on or before 1st December of each year. Newly licensed stablecoin issuers must pay BD 5,000 towards licensing fee at the time of grant of license and for the first full year of operation, licensees must pay the minimum fee of BD 5,000. For subsequent years, the stablecoin issuer must submit the 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).**

SIO-2.4.2 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.

SIO-2.4.3 **Operating expenses are defined as the total operating expenses of the stablecoin issuer, as per the audited financial statements of the preceding year, subject to the exclusion of the following items from the operating expenses**
(a) Training costs;
(b) Charitable donations;
(c) CBB fees paid;
(d) Non-executive Directors' remuneration;
(e) Depreciation;
(f) Provisions;
(g) Interest expense; and
(h) Dividends

SIO-2.4.4 The CBB would normally rely on the audited accounts of a stablecoin issuer 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.

SIO-2.4.5 **Stablecoin issuers 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.**

SIO-2.4.6 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.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-3	Licensing Conditions

SIO-3.1 Licensing Conditions

SIO-3.1.1 **A stablecoin issuer must be ensure it meets the following conditions:**

Condition: 1: Legal form

(a) Locally incorporated as a Bahraini Joint Stock Company (BSC);

Condition 2: Substantial shareholder

(b) Any persons holding 5% or more of the shareholding or in a position to control not less than 5% of the shareholder votes in the licensee are suitable and pose no undue risks to the stablecoin issuer;

Condition 3: Mind management

(c) Collectively provide sufficient range of skills and experience to manage the affairs of the stablecoin issuer in a sound and prudent manner. Stablecoin issuers must ensure their employees meet any training and competency requirements specified by the CBB;

(d) Ensure that adequate level of seniority for personnel undertaking the following functions, all of which must be approved by the CBB prior to their appointment (See also Form 3):

- **i. Chief Executive Officer or General Manager;**
- **ii. Compliance Officer;**
- **iii. Money Laundering Reporting Officer;**
- **iv. Head of Risk Management;**
- **v. Head of Reserve Asset Management;**
- **vi. Head of Operations; and**
- **vii. Chief Information Security Officer;**

Condition 4: Adequate financial resources

(e) Maintain a level of financial resources, as agreed with the CBB, adequate for the level of business proposed. The level of financial resources held must always equal or exceed the minimum requirements contained in Chapter 4 of this Module;

Condition 5: Systems and Controls

(f) Maintain systems and controls that are adequate for the scale and complexity of their activities. These systems and controls, at a minimum, must meet the requirements stipulated in this Module as well as the requirements of Module HC (High Level Controls) of the CBB Rulebook Volume 6;

Condition 6: Auditors

(g) Appoint an external auditor, subject to CBB's prior approval. Stablecoin issuers must comply with the minimum requirements regarding auditors contained in Section SIO-5.2 of this Module;

SIO-3.1 Licensing Conditions (continued)

Condition 7: Books and records

(h) 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. Stablecoin issuers must ensure that all relevant books and other information, as may be required by the CBB, are kept for a minimum period of 10 years;

Condition 8: Conduct

(i) Conduct their activities in a professional and orderly manner, in keeping with good market practice standards. Stablecoin issuers must comply with the general standards of business conduct as well as the standards relating to treatment of clients contained in this Module;

SIO-3.1.2 **Stablecoin issuers must comply with any other specific requirements or restrictions imposed by the CBB on the scope of their license.**

.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-4	Financial Resources Requirement

SIO-4.1 Initial Paid-Up Capital (Base Capital) Requirement

SIO-4.1.1 The minimum initial paid-up share capital (base capital) for grant of stablecoin issuer license is BHD 250,000.

SIO-4.1.2 Applicants are required to ensure that the minimum initial paid-up share 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.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-4	Financial Resources Requirement

SIO-4.2 Prudential Requirements

SIO-4.2.1 **A stablecoin issuer must, at all times, have as net shareholders equity equal to higher of the following:**

(a) the initial paid-up share capital (base capital) requirement referred to in Paragraph SIO-4.1.1; or

(b) the par value capital requirement referred to in Paragraph SIO-4.2.2; and

Par Value Capital Requirement

SIO-4.2.2 **For the purposes of Paragraph SIO-4.2.1(b), stablecoin issuers must determine the par value capital which is equal to:**

Par value capital = 2% of the average par value of approved stablecoin in circulation

SIO-4.2.3 For avoidance of doubt, average par value means the par value of an approved stablecoin in circulation at the end of each calendar day, calculated over the preceding six months. When a stablecoin issuer offers more than one approved stablecoin, the par value capital requirement shall be the sum of the average of the par value capital requirement for each approved stablecoin.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-4	Financial Resources Requirement

SIO-4.3 Minimum Liquid Fund Requirement

SIO-4.3.1 **Stablecoin issuers must maintain an amount equal to one quarter of the preceding year's aggregate fixed overheads in liquid assets, reviewed annually.**

SIO-4.3.2 **For the purposes of Paragraph SIO-4.3.1, stablecoin issuers must calculate their fixed overheads for the preceding year, by subtracting the following items from the total expenses after distribution of profits to shareholders in their most recently audited annual financial statements:**

- **(a) staff bonuses and other remuneration, to the extent that those bonuses and that remuneration depend on a net profit of the licensed stablecoin issuer in the relevant year;**
- **(b) employees, directors and partners share in profit;**
- **(c) other appropriations of profits and other variable remuneration, to the extent that they are fully discretionary**
- **(d) non-recurring expenses from non-ordinary activities.**

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-4	Financial Resources Requirement

SIO-4.4 Additional Capital Requirement

SIO-4.4.1 **The CBB may, at its sole discretion, require a stablecoin issuer to hold an amount of capital which is up to 50% higher than the amount resulting from the application of Paragraph SIO-4.2.1, where an assessment of any of the following indicates a higher degree of risk:**

(a) the evaluation of the risk-management processes and internal control mechanisms of the stablecoin issuer of the approved stablecoin;

(b) the quality and volatility of the reserve assets referred to in Chapter 6 of this Module;

(c) the types of rights granted by the stablecoin issuer to the clients holding approved stablecoins in accordance with Section SIO-6.5 (permanent right of redemption);

(d) the stablecoin is classified as a significant stablecoin.

SIO-4.4.2 The CBB, while undertaking the risk assessment mentioned in Paragraph SIO-4.4.1, shall apply the following criteria:

(a) whether the stablecoin issuer is likely to breach the requirements referred to in Chapter 6 of this Module (Reserve assets and Redemption Requirement) and Section SIO-5.3 (Governance Requirements) of Chapter 5 within the following 12 months;

(b) whether at all times redemption at par value is not ensured either in normal or in stressed market condition;

(c) whether there is an increased risk of a significant deteriorate on the value of the reserve assets or the financial condition of the stablecoin issuer; and

(d) whether there is an increased risk arising from systems including the underlying distributed ledger and any trading platform or payment system used for the issuance or the transfer of the approved stablecoin and from other third-party crypto asset service providers such as custodians to which the approved stablecoin and/or reserve asset might rely on.

SIO-4.4.3 While assessing a stablecoin issuer for additional capital requirement provided for in Paragraph SIO-4.4.1, the CBB shall perform the evaluation on a case-by-case basis following a broad assessment of all the criteria specified in Paragraph SIO-4.4.1. A stablecoin issuer shall be subjected to additional capital requirement only when there is a high degree of risk, which is not already covered, and the measures taken by the stablecoin issuer are insufficient to effectively reduce the risks.

SIO-5.1 General Obligations

SIO-5.1.1 In the course of undertaking regulated stablecoin offering service, a stablecoin issuer must:

Dealing with clients and other stakeholders

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

(b) Stablecoin issuers must act honestly, fairly and professionally and communicate with their clients and prospective clients in a fair, clear and not misleading manner; and

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

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

(e) 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;

(f) 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;

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

(h) Not act contrary to the interests of its clients;

(i) Stablecoin issuers must act in the best interests of their clients and treat them equally;

(j) Take appropriate measures to safeguard any money and approved stablecoin handled on behalf of clients and maintain confidentiality of client information;

Risk management

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

Internal operating policies and procedures

(l) Have an operating manual and internal policies;

Compliance

(m) Maintain proper arrangements to enforce compliance with the CBB Law, Rules and Regulations and develop, implement, and adhere to a "compliance policy", tailored to meet specific requirements associated with regulated stablecoin offering services. The compliance policy must reflect a clear comprehension and understanding of compliance responsibilities with respect to approved stablecoins;

Training and skills

(n) Ensure that all the employees are provided with the required education, qualifications and experience and they fully understand the rules and regulations of the CBB;

Record keeping

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

Shareholder meetings

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

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

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

(s) Within one month of any shareholders meetings referred to in Paragraph SIO-5.1.1(o), provide to the CBB a copy of the minutes of the meeting.

SIO-5.1.2 A stablecoin issuer 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.

SIO-5.1.3 A stablecoin issuer 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 custodian firms outside of Bahrain (not licensed by the CBB) about any associated risks.

SIO-5.1.4 Where a stablecoin issuer holds their own approved stablecoins, either due to redemption or due to minting, such approved stablecoins must be fully backed by the reference fiat currency.

SIO-5.2 Auditors and Accounting Standards

SIO-5.2.1 **Stablecoin issuers must appoint an independent external auditor for its accounts for every financial year. While appointing an auditor, stablecoin issuers must exercise due skill, care and diligence in the selection and appointment of the auditor and must take into consideration the auditor's experience and track record of auditing stablecoin and/or crypto-asset related businesses.**

SIO-5.2.2 In accordance with Article 61(b) of the CBB Law, if a stablecoin issuer fails to appoint an auditor within four months from the beginning of its financial year, the CBB shall appoint an auditor on behalf of the stablecoin issuer.

SIO-5.2.3 **A stablecoin issuer must pay the fees of the auditor regardless of the manner in which the auditor is appointed.**

SIO-5.2.4 **An auditor must not be the chairman or a director in the stablecoin issuer's board or a managing director, agent, representative or taking up any administrative work therein, or supervising its accounts, or a next of kin to someone who is responsible for the administration or accounts of the stablecoin issuer or having an extraordinary interest in the stablecoin issuer.**

SIO-5.2.5 **If any of the circumstances referred to in rule Paragraph SIO-5.2.4 occurs after the appointment of the auditor, the stablecoin issuer must appoint another external auditor.**

SIO-5.2.6 **Licensed stablecoin issuers must provide the external auditor with all information and assistance necessary for carrying out his duties.**

SIO-5.2.7 **The duties of the external auditor must include the preparation of a report on the final accounts. The report must contain a statement on whether the stablecoin issuer's accounts are correct and reflect the actual state of affairs of the licensee according to the auditing standards prescribed by the CBB, and whether the stablecoin issuer has provided the auditor with all required information and clarifications.**

SIO-5.2.8 **The final audited accounts must be presented to the general meeting of the licensed stablecoin issuer together with the auditor's report. A copy of these documents must be sent to the CBB at least 15 days before the date of the general meeting.**

SIO-5.2.9 **Audited financial statements of a stablecoin issuer must be prepared in accordance with the International Financial Accounting Standards (IFRS) or AAOIFI standards as appropriate.**

SIO-5.2 Auditors and Accounting Standards (continued)

Annual Audited Financial statements

SIO-5.2.10 Stablecoin issuers 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

SIO-5.2.11 Stablecoin issuers must submit a soft copy (electronic) of their full annual report to the CBB within 4 months of the end of their financial year.

Reviewed (Unaudited) Quarterly Financial Statements

SIO-5.2.12 Stablecoin issuers must submit to the CBB unaudited quarterly financial statements (in the same format as their Annual Audited Accounts), reviewed by the licensee's external auditor, on a quarterly basis within 45 calendar days from the end of each of the first 3 quarters of their financial year.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-5	Business Standards & Ongoing Obligations

SIO-5.3 Governance Requirements

SIO-5.3.1 A stablecoin issuer must have robust governance arrangements, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks to which they are or might be exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures.

SIO-5.3.2 Stablecoin issuers must adopt policies and procedures that are sufficiently effective to ensure compliance with the requirements of this Module and other applicable Modules. Stablecoin issuer must establish, maintain and implement, in particular, policies and procedures on:

(a) the reserve assets referred to in Section SIO-6.1, Section SIO-6.2 & Section SIO-6.3;
(b) the custody of the reserve assets, including the segregation of assets, as specified in Section SIO-6.4;
(c) the rights granted to the holders of approved stablecoins, as specified in Section SIO-6.5;
(d) the mechanism through which approved stablecoins are issued and redeemed;
(e) the protocols for validating transactions in approved stablecoins;
(f) the functioning of the stablecoin issuer's proprietary distributed ledger technology, where the approved stablecoins are issued, transferred and stored using such distributed ledger technology or similar technology that is operated by the stablecoin issuer or a third party acting on their behalf;
(g) the mechanisms to ensure the liquidity of approved stablecoins, including the liquidity management policy and procedures for issuers of significant stablecoins referred to in Section SIO-8.2.5(b);
(h) arrangements with third-party entities for managing the reserve assets, and for the investment of the reserve assets, the custody of the reserve assets and, where applicable, the distribution of the approved stablecoins to the public;
(i) the written consent of the stablecoin issuer given to third parties that might offer or seek the admission to trading of the approved stablecoin;
(j) complaints-handling, as specified in Section SIO-5.8;
(k) conflicts of interest, as specified in Section SIO-5.9;

SIO-5.3 Governance Requirements (continued)

SIO-5.3.3 For the purposes of Paragraph SIO-5.3.2(h), stablecoin issuers must enter into a written contact with the third party. The contractual arrangements must set out the roles, responsibilities, rights and obligations both of the licensee and of the third party. Any contractual arrangement with cross jurisdictional implications must provide for an unambiguous choice of applicable law.

SIO-5.3.4 Unless a stablecoin issuer initiates a redemption plan referred to in Chapter 11 of this Module, the stablecoin issuer must employ appropriate and proportionate systems, resources and procedures to ensure the continued and regular performance of their services and activities. To this end, stablecoin issuers must maintain all of their systems and security access protocols in conformity with necessary and appropriate standards.

SIO-5.3.5 Where a stablecoin issuer decides to discontinue the provision of its regulated stablecoin offering services and activities, including by discontinuing the offering of a particular approved stablecoin, it must submit a plan to the CBB for approval of such discontinuation.

SIO-5.3.6 Stablecoin issuers must identify sources of operational risk and minimise those risks through the development of appropriate systems, controls and procedures.

SIO-5.3.7 Stablecoin issuers must establish a business continuity policy and plans to ensure, in the case of an interruption of their ICT systems and procedures, the preservation of essential data and functions and the maintenance of their activities or, where that is not possible, the timely recovery of such data and functions and the timely resumption of their activities.

SIO-5.3.8 Stablecoin issuers must have in place internal control mechanisms and effective procedures for risk management, including effective control and safeguard arrangements for managing ICT systems. Further, stablecoin issuers must monitor and evaluate on a regular basis the adequacy and effectiveness of the internal control mechanisms and procedures for risk assessment and take appropriate measures to address any deficiencies in that respect.

SIO-5.3.9 Stablecoin issuers must have systems and procedures in place that are adequate to safeguard the availability, authenticity, integrity and confidentiality of data as required under Personal Data Protection Law. Those systems must record, and safeguard relevant data and information collected and produced in the course of the stablecoin issuer's activities.

SIO-5.3 Governance Requirements (continued)

Responsibility of the Board of Directors

SIO-5.3.10 The Board of a stablecoin issuer is responsible for overseeing the implementation of sound governance arrangements that ensure effective and prudent management of the licensee and the interest of its clients including the segregation of duties and the identification, prevention and management of conflicts of interest.

SIO-5.3.11 The Board must establish and approve:

(a) the overall business strategy and the key policies of the stablecoin issuer taking into account the licensee's long-term financial interests and solvency and interest of the clients;
(b) the policies required under Paragraph SIO-5.3.3 and such policies must be consistent with the risk appetite the stablecoin issuer;
(c) the organisation structure of the stablecoin issuer;
(d) the overall risk strategy, the stablecoin issuer's risk appetite and its risk management framework;
(e) an effective internal control framework to ensure compliance with applicable regulatory requirements including with regard to the management of reserve assets;
(f) in accordance with the requirement of Paragraph SIO-8.2.5(a), a remuneration policy applicable upon classification of an approved stablecoin as significant stablecoin;
(g) the policies and procedures to identify, prevent, manage and disclose conflicts of interest, in line with Section SIO-5.9;
(h) arrangements that aim to ensure the integrity of the accounting and financial reporting systems, including financial and operational controls and compliance with the law and relevant standards.

SIO-5.3.12 The Board must assess and periodically review the effectiveness of the policy arrangements and procedures put in place to comply with Chapters 5,6,8 and 11 of this Module and take appropriate measures to address any deficiencies.

Responsibility of Senior Management

SIO-5.3.13 The senior management is responsible for the implementation of the strategies and policies set out by the Board and must regularly discuss the implementation and appropriateness of these strategies and policies with the Board.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-5	Business Standards & Ongoing Obligations

SIO-5.3 Governance Requirements (continued)

SIO-5.3.14 The senior management must:

(a) actively engage in the business of the stablecoin issuer and must take decisions on a sound and well-informed basis.

(b) monitor that the risk culture of the licensee is implemented consistently;

(c) oversee the implementation of policies and procedures to identify, prevent, manage and disclose conflicts of interest, in accordance with Section SIO-5.9 of this Module;

(d) oversee the integrity of financial information and reporting, and the internal control framework, including an effective and sound risk management framework;

(e) ensure that the heads of internal control functions are able to act independently and, regardless of the responsibility to report to other business lines or units, can raise concerns and warn the management body in its supervisory function directly, where necessary, when adverse risk developments affect or may affect the stablecoin issuer; and

(f) set and monitor the implementation of the internal audit plan.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-5	Business Standards & Ongoing Obligations

SIO-5.4 Internal Control

Internal Control Framework

SIO-5.4.1 Stablecoin issuers must develop and maintain an internal control framework tailored to the specificity of the licensee's business, its complexity, and the associated risks.

SIO-5.4.2 The internal control framework must cover the whole organisation, including the Board and senior management responsibilities and tasks, and the activities of all business lines and internal departments, including internal control functions and the use of third-party service providers.

SIO-5.4.3 The internal control framework of a stablecoin issuer must ensure:
(a) effective and efficient operations including with regard to issuance of stablecoins;
(b) adequate identification, measurement and mitigation of risks including operational risk and risk related to ICT;
(c) the reliability of financial and non-financial information reported both internally and externally;
(d) sound administrative and accounting procedures; and
(e) compliance with laws, regulations, supervisory requirements and the stablecoin issuer's internal policies, processes and rules.

Internal Control function

SIO-5.4.4 The internal control framework referred to in Paragraph SIO-5.4.1 requires establishment of internal control function. The internal control function, at a minimum, must include a permanent and effective compliance function with appropriate and sufficient authority. Stablecoin issuers may, based on the principle of proportionality and commensurate to its size, internal organisation, business model, and nature, scale and complexity of its business activities, include the internal risk management function and internal audit function within the internal control functions.

SIO-5.4.5 Stablecoin issuers must, prior to implementation of the internal control framework, provide details of the internal control framework and internal control function to the CBB.

SIO-5.4 Internal Control (continued)

Heads of Internal Control Function

SIO-5.4.6 Heads of internal control function must be established at an adequate hierarchical level that provides the head of the internal control function with the appropriate authority to fulfil his or her responsibilities. The head of compliance, the heads of the risk management and internal audit functions should have access to the Board. This should not prevent the heads of internal control function from reporting within the regular reporting lines as well.

Independence of Internal Control Functions

SIO-5.4.7 The internal control function must operate in an independent manner without being subject to any form of internal or external influence. In order to ensure independence, stablecoin issuers must take necessary measures which should include amongst others;

(a) Staffs who are part of the internal control functions do not perform any operational tasks that fall within the scope of the activities the internal control functions are intended to monitor and control;

(b) the remuneration of the internal control functions staff must not be linked to the performance of the activities the internal control function monitors and controls and must not otherwise be likely to compromise the staff members objectivity;

(c) where appropriate, the staff are organisationally separate from the activities they are assigned to monitor and control.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-5	Business Standards & Ongoing Obligations

SIO-5.5 Compliance Function

SIO-5.5.1 **Stablecoin issuers must establish a permanent and effective compliance function to manage compliance risk and appoint a competent person as compliance officer.**

SIO-5.5.2 Stablecoin issuers may combine the position of compliance officer with the money laundering reporting officer provided there is no conflict of interest between the tasks performed and the size, internal organisation, business model, and nature, scale and complexity of the licensee's activities is such that the licensee can effectively meet the regulatory requirements.

SIO-5.5.3 **Stablecoin issuers must seek the CBB's prior written before combining the position of head of functions referred to in Paragraph SIO-5.5.2.**

SIO-5.5.4 **Employees within the compliance function must possess sufficient knowledge, skills and experience in relation to compliance and relevant procedures and should undergo regular training.**

SIO-5.5.5 **Stablecoin issuers must have a well-documented compliance policy, and the senior management must oversee the implementation of the compliance policy. Stablecoin issuers must set up a process to regularly assess changes in the law and regulations applicable to its business activities.**

SIO-5.5.6 The compliance function should advise the board and senior management body on measures to be taken to ensure compliance with applicable laws, rules, regulations and standards, and should assess the possible impact of any changes in the legal or regulatory environment on the stablecoin issuer's activities and compliance framework.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-5	Business Standards & Ongoing Obligations

SIO-5.6 Internal Audit Function

SIO-5.6.1 The internal audit function must be independent and have sufficient authority and resources. In particular, stablecoin issuers must ensure that the qualification of the internal audit staff members and the internal audit resources, in particular its auditing tools and risk analysis methods, are adequate for the nature, scale and complexity of the risks associated with the licensed stablecoin issuer's business model, activities, and risk appetite.

SIO-5.6.2 The internal audit function must follow a risk-based approach, independently review and provide objective assurance of the compliance of all activities undertaken by the stablecoin issuer, including the use of third-party entities, with the licensee's policies and procedures and with the regulatory requirements.

SIO-5.6.3 The internal audit function must not be involved in designing, selecting, establishing, or implementing specific internal control policies, mechanisms, procedures or risk limits. However, this should not prevent the Board and the senior management from requesting input from the internal audit function on matters relating to risk, internal controls and compliance with applicable rules.

SIO-5.6.4 The internal audit function must review the adequateness of the processes for the development of stablecoin whitepaper, its approval and the processes followed for issuance of the approved stablecoin and how the approved stablecoin is offered to the public.

SIO-5.6.5 Internal audit work should be performed regularly in accordance with an audit plan and a detailed audit programme following a risk-based approach.

SIO-5.6.6 Stablecoin issuers must, at least once a year, draw up an internal audit plan on the basis of the annual internal audit control objectives. The internal audit plan must be approved by the senior management.

SIO-5.7 Marketing & Promotion (continued)

(a) The relevant material information, including providing clients with access to up-to-date stablecoin whitepaper or information, and providing clients with material information as soon as reasonably practicable to enable clients to appraise the position of their investments (for example, any major events or any other material information);

(b) Circumstances under which the stablecoin issuer may disclose the client's confidential information to third parties, including regulators;

(c) Client's right to prior notice of any change in the stablecoin issuer's rules, policies and terms and conditions;

(d) Dispute resolution mechanisms, including complaints procedures; and

(e) System upgrades and maintenance procedures and schedules.

SIO-5.8 Complaints

SIO-5.8.1 Stablecoin issuers must establish and maintain written policies and procedures to resolve complaints in a fair and timely manner.

SIO-5.8.2 Stablecoin issuers must provide, in a clear and conspicuous manner on their website and in all physical locations the following disclosures:

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

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

SIO-5.8.3 Stablecoin issuers must notify the CBB any change in their complaint policies or procedures within seven days prior to the implementation of the new complaint policy.

SIO-5.8.4 The complaint handling procedures of a stablecoin issuer must provide for:

(a) The receipt of written complaints;

(b) The appropriate investigation of complaints;

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

(d) Notification of the decision to the client;

(e) The recording of complaints; and

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

SIO-5.8.5 A stablecoin issuer's internal complaint handling procedures must be designed to ensure that:

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

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

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

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

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

Response of Complaints

SIO-5.8.6 Stablecoin issuer must acknowledge in writing clients written complaints within 5 working days of receipt.

SIO-5.8 Complaints (continued)

SIO-5.8.7 A stablecoin issuer must respond to a client complaint promptly and within a period of 4 weeks of receiving the complaint or provide the complainant with an appropriate explanation as to why the licensee is not, at that time, in a position to respond and must indicate by when the licensee will respond.

Redress

SIO-5.8.8 A stablecoin issuer must decide and communicate how it proposes to provide the customer with redress. Where appropriate, the licensee must explain the options open to the customer and the procedures necessary to obtain the redress.

SIO-5.8.9 Where a stablecoin issuer decides that redress in the form of compensation is appropriate, the licensee must provide the complainant with fair compensation and must comply with any offer of compensation made by it which the complainant accepts.

SIO-5.8.10 Where a stablecoin issuers decides that redress in a form other than compensation is appropriate, it must provide the redress as soon as practicable.

SIO-5.8.11 Stablecoin issuers must inform the clients who have filed a complaint with the licensee and are not satisfied with the response received as per Paragraph SIO-5.8.7, about their right to forward the complaint to the Consumer Protection Unit at the CBB within 30 calendar days from the date of receiving the letter from the licensee.

Reporting of Complaints

SIO-5.8.12 Stablecoin issuers must submit to the Consumer Protection Unit at the CBB, a quarterly report summarising the following:

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

SIO-5.8.13 Where no complaints have been received by the stablecoin issuer within the quarter, a 'nil' report must be submitted to the Consumer Protection Unit at the CBB.

SIO-5.8 Complaints (continued)

Record of Complaints

SIO-5.8.14 Stablecoin issuers must maintain a record of all the client complaints received. The record of each complaint must include:

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

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

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-5	Business Standards & Ongoing Obligations

SIO-5.9 Conflict of Interest

SIO-5.9.1 **Stablecoin issuers must implement and maintain effective policies and procedures to identify, prevent, manage and disclose conflicts of interest between themselves and:**
(a) their shareholders;
(b) their senior management & employees;
(c) their clients; or
(d) any third party providing custody and management of reserve assets.

SIO-5.9.2 **The conflict of interest policies referred to in Paragraph SIO-5.9.1 must address all such situations which may influence or affect, or which may be perceived to influence or affect, the stablecoin issuer's ability or the ability of any person connected to the licensee such as its shareholders, board of directors, senior management, employees etc., to take impartial and objective decisions. In particular, the conflict of interest policies and procedures must specifically cover:**
(a) conflicts that may impede the ability of the senior management to take objective and impartial decisions that aim to be in the best interest of the stablecoin issuer without prejudice to the consideration of interests of the clients;
(b) potential conflict of interest situation that may arise from the management and investment of reserve assets.

SIO-5.9.3 **The conflict of interest policies and procedures must, at a minimum include:**
(a) a description of the circumstances which may give rise to a conflict of interest situation particularly with reference to the scenarios referred to in Paragraph SIO-5.9.4 and Paragraph SIO-5.9.6;
(b) the policies and procedures to be adopted in order to prevent or manage, and disclose, such conflicts. The policies and procedures should differentiate between conflicts of interest that persist and need to be managed permanently and conflicts of interest that occur with regard to a single event for which a one-off measure can be appropriate.

Conflict of interest potentially detrimental to the clients

SIO-5.9.4 For the purposes of identifying the types of conflicts of interest that arise in the course of issuing, processing and redeeming approved stablecoins or of investing or managing the reserve assets and whose existence may damage the interests of the clients, stablecoin issuers should take into account, whether the licensee, shareholders, board of directors, senior management, employees and third parties providing custody and management of reserve asset service is in any of the following situations:

SIO-5.9 Conflict of Interest (continued)

(a) is likely to make a financial gain, avoid a financial loss, or receive another kind of benefit, at the expense of the clients;
(b) it has an interest in the outcome of an activity carried out to the benefit of the client, including the redemption of the approved stablecoin, which is distinct from the interest of the client.

SIO-5.9.5 For the purposes of identifying the types of conflicts of interest that arises in the course of managing the reserve assets, the stablecoin issuer shall assess whether it receives or will receive an inducement in relation to that activity in the form of monetary or non-monetary benefits or services in a way that may damage the interest of the client.

Conflicts of interest potentially detrimental to the stablecoin issuers

SIO-5.9.6 For the purposes of identifying the circumstances which could adversely influence the performance of a shareholder, board of director, senior management, employee and third party providing custody and management of reserve asset, in particular when investing and managing the reserve assets, stablecoin issuers should take into account situations or relationships where the aforementioned person:
(a) has an economic interest in a person, body or entity with interests conflicting with those of the licensee;
(b) has or has had within at least the last 3 years a personal relationship with a person, body or entity with interests conflicting with those of the licensee;
(c) has or has had within at least the last 3 years a professional relationship with a person, body or entity with interests conflicting with those of the licensee;
(d) has or has had within at least the last 3 years a political relationship with a person, body or entity with interests conflicting with those of the licensee;
(e) carries out conflicting activities, is entrusted with conflicting responsibilities.

SIO-5.9.7 For the purposes of identifying the persons, bodies or entities with conflicting interests, as set out in Paragraph SIO-5.9.6, stablecoin issuers should take into account whether that person, body or entity is in any of the following situations:
(a) it is likely to make a financial gain, or avoid a financial loss, at the expense of the licensee;
(b) it has an interest in the outcome an activity carried out or a decision taken by the stablecoin issuer, which is distinct from the licensee's interest in that outcome;
(c) it carries out the same business as the stablecoin issuer or is a client, consultant, service providers or other supplier of the licensee.

SIO-5.9.8 For the purposes of Paragraph SIO-5.9.6(a), stablecoin issuers should take into account the following situations or relationships where a shareholder, board of director, senior management, employee and third party providing custody and management of reserve asset:
(a) holds shares, tokens (including governance tokens), other ownership rights or membership in that person, body or entity;

SIO-5.9 Conflict of Interest (continued)

(b) holds debt instruments of or has other debt arrangements with that person, body or entity;

(c) has any form of contractual arrangements, such as management contracts, service contracts, delegation or outsourcing contract or intellectual property licenses, with that person, body or entity.

Remuneration procedures, policies and arrangements

SIO-5.9.9 **Stablecoin issuers must within their policies and procedures ensure that remuneration procedures, policies and arrangements:**

(a) do not create a conflict of interest or provide for incentives in the short, medium or long term that may lead the employees or members of the senior management to favour their own interests or the stablecoin issuer's interests to the potential detriment of any client or shareholders of the licensee.

(b) identify and appropriately mitigate conflicts of interest potentially caused by the award of variable remuneration, underlying key performance indicators and risk alignment mechanisms, including the pay out of instruments to employees or senior management as part of the variable or fixed remuneration.

Disclosure of Conflict of Interest

SIO-5.9.10 **Stablecoin issuers must, in a prominent place on their website, disclose to their clients the general nature and sources of conflicts of interest referred to in Paragraph SIO-5.9.1 and the steps taken to mitigate them. The aforementioned disclosure must contain:**

(a) the circumstances giving rise, or which may give rise to conflicts of interest of the kind referred to in Paragraph SIO-5.9.4 and Paragraph SIO-5.9.6, including the role and capacity in which the licensee is acting in relation to the client;

(b) the nature of the conflicts of interest identified;

(c) the associated risks identified in relation to the conflicts of interest referred to in (a) above; and

(d) the steps and measures taken to prevent or mitigate the identified conflicts of interest.

SIO-5.9.11 **Stablecoin issuers must not construe the disclosure of conflict of interest, referred to in Paragraph SIO-5.9.10, as a means or a way to manage and mitigate conflicts of interest.**

SIO-5.9 Conflict of Interest (continued)

Personal Transactions

SIO-5.9.12 Stablecoin issuers must establish, implement and maintain adequate arrangements aimed at ensuring that personal transactions are identified or notified before a decision is taken, documented and that decisions to enter into personal transactions are taken objectively, in the interest of each party, and shall correspond to the conditions that would have applied between independent parties for the same transactions in the absence of a conflict of interest.

SIO-5.9.13 The arrangements referred to in Paragraph SIO-5.9.12 must be designed to ensure that:

(a) the applicable decision making processes for entering into personal transactions is set out. The stablecoin issuer must set appropriate thresholds (per transaction or depending on the conditions) above which the personal transaction requires the approval of senior management;

(b) each relevant person is aware of the rules applied on personal transactions, and of the measures established by the licensee in connection with personal transactions;

(c) the stablecoin issuer is informed promptly of any personal transaction entered into by a relevant person, either by notification of that transaction or by other procedures enabling the licensee to identify such transactions;

(d) a record and documentation is kept of the personal transaction notified to the stablecoin issuer or identified by it, including any authorisation or prohibition in connection with such a transaction.

SIO-5.9.14 For the purposes of Paragraph SIO-5.9.12, a transaction shall be considered as a personal transaction when there is an exchange of approved stablecoin issued by the stablecoin issuer for fiat currency or a redemption of approved stablecoin and is carried out from the account of any of the following relevant persons;

(a) Shareholder;
(b) Board of Director;
(c) Senior Management and Employees; and
(d) Third parties providing custody and management of reserve assets;

For avoidance of doubt, transactions done by aforementioned persons through the accounts of their spouse(s), children(s) or any other account(s) in which the relevant person holds any beneficial interest shall also be considered as personal transaction.

SIO-5.10 Anti Money Laundering and Combating the Financing of Terrorism

SIO-5.10.1 Stablecoin issuers must have adequate and appropriate systems and controls, in accordance with the requirements of Anti Money Laundering and Combating of Financial Crime (AML) Module, CBB Rulebook Volume 6, to prevent, detect and combat money laundering and terror financing.

SIO-5.10.2 The AML/CFT systems and controls referred to in Paragraph SIO-5.10.1 must include but not be limited to (i) customer due diligence in relation to the offering and redemption of the approved stablecoin, (ii) transaction monitoring and (iii) crypto asset transfer (travel rule) and wire transfer rules as provided for in AML-2A of the Anti-Money Laundering and Combating of Financial Crime (AML) Module, CBB Rulebook Volume 6.

SIO-5.10.3 For avoidance of doubt, stablecoin issuers must ensure that clients making redemption request are compliant with the customer due diligence requirements prior to processing of the redemption request.

SIO-6.1 Reserve Asset Composition and Management

SIO-6.1.1 **Stablecoin issuers, at all times, must hold and maintain sufficient reserve assets such that the value of the reserve assets must be equivalent to at least one hundred percent (100%) of the par value of the outstanding approved stablecoins in circulation, including those held by the licensee.**

SIO-6.1.2 **Stablecoin issuers must ensure that the reserve assets held are:**

(a) denominated in the same reference currency as the pegged currency i.e. the fiat currency backing the approved stablecoin (except for Bahraini Dinar denominated stablecoin);

(b) sufficient in value to back each one of the approved stablecoins issued;

(c) stable in value; and

(d) sufficiently liquid to meet the permanent right of redemption of the clients.

SIO-6.1.3 **For the purposes of Paragraph SIO-6.1.1, stablecoin issuers must ensure that the reserve assets are valued on a daily basis by using their current market value i.e. the reserve assets are marked to market on daily basis for the purpose of valuation.**

SIO-6.1.4 When using mark-to-market valuation the reserve assets must be valued at the prudent side of the bid and offer unless the reserve assets can be closed out at mid-market value. Only market data of good quality should be used, and data should be assessed on all of the following factors:

(a) the number and quality of counterparties;

(b) the volume and turnover in the market of the reserve asset;

(c) the total size of the reserve asset**.**

SIO-6.1.5 Where use of mark-to-market as referred to Paragraph SIO-6.1.3 is not possible or the market data is not of sufficiently good quality, the reserve asset must be valued conservatively by using mark-to-model. The model should accurately estimate the intrinsic value of the reserve asset, based on all of the following up-to-date key factors:

(a) the volume and turnover in the market of that reserve asset;

(b) the total size of the reserve asset;

(c) the market risk, interest rate risk and credit risk attached with the reserve asset.

Composition of Reserve Assets

SIO-6.1.6 **Stablecoin issuers must ensure that the reserve assets are of high quality and high liquidity with minimal market, credit and concentration risk. In determining the composition of the reserve assets, stablecoin issuers must take into account the liquidity requirements of the approved stablecoin under consideration and how the reserve assets will be managed and invested without any risk to clients permanent right of redemption.**

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-6	Reserve Asset & Redemption Right

SIO-6.1 Reserve Asset Composition and Management (continued)

SIO-6.1.7 Stablecoin issuers must ensure that the composition of reserve asset only includes the following: :

(a) Cash and deposits held with banks rated at a minimum AA- or equivalent;
(b) Debt securities with residual maturity of 90 days or less issued by the central bank of the reference currency;
(c) Repurchase agreement with a maturity of 7 days or less which are backed by (c) above; and
(d) Short term government money market funds.

SIO-6.1.8 In addition to the requirement of Paragraph SIO-6.1.7, stablecoin issuers issuing Bahraini Dinar (BHD) backed approved stablecoins can invest in US Dollar (USD) denominated T-bills with residual maturity of 90 days or less and issued by the central bank of the reference currency.

Segregation of Reserve Assets

SIO-6.1.9 Stablecoin issuers must put in place effective arrangement to ensure that the:

(a) reserve assets are legally segregated from the licensee's own assets so that creditors of the stablecoin issuers have no recourse to the reserve assets in the event of insolvency; and
(b) reserve assets are operationally segregated from the stablecoin issuer's own assets.

SIO-6.1.10 Stablecoin issuers that offer two or more approved stablecoins must operate and maintain segregated pools of reserves assets for each approved stablecoin. Each of those pools of reserves assets must be managed separately.

SIO-6.1.11 Stablecoin issuers must put in place effective internal control measures and procedures to protect the reserve assets from operational risks, including the risks of theft, fraud and misappropriation.

SIO-6.1.12 Stablecoin issuers must put in place an investment policy for the reserve assets which should be reviewed for suitability on an annual basis or more frequently depending on the nature, size and complexity of the business.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-6	Reserve Asset & Redemption Right

SIO-6.1 Reserve Asset Composition and Management (continued)

SIO-6.1.13 Stablecoin issuers must appoint a qualified person as head of reserve asset management with appropriate authority to implement the investment policy referred to in Paragraph SIO-6.1.12. The appointed approved person shall be responsible for effective implementation of the investment policy.

SIO-6.1.14 Stablecoin issuers must ensure that the issuance and redemption of approved stablecoin is always matched by a corresponding increase or decrease in the reserve assets.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-6	Reserve Asset & Redemption Right

SIO-6.2 Audit Requirements of Reserve Assets

SIO-6.2.1 Stablecoin issuers must, on a monthly basis, obtain a report by an independent external audit firm confirming the following:

a. the approved stablecoin is one hundred percent backed by reserve assets;
b. the number and market value of approved stablecoin in circulation; and
c. the composition and value of the reserve assets.

SIO-6.2.2 The report referred to in Paragraph SIO-6.2.1 must be submitted to the CBB and published on the stablecoin issuer's website by the end of the following month for the month being reported.

SIO-6.3 Reconciliation and Addressing Discrepancies

Reconciliation

SIO-6.3.1 Stablecoin issuers must conduct internal and external reconciliation on a daily basis. For internal reconciliation, stablecoin issuers must compare, as per their own records, the value of reserve assets against the par value of the approved stablecoins in circulation and check whether the value matches. For external reconciliation, stablecoin issuers must compare their internal records of reserve asset valuation and par value of approved stablecoins in circulation with the records of any third party with whom the reserve assets are being held and the approved stablecoins are being held.

Addressing Discrepancies: Excess

SIO-6.3.2 Upon daily valuation and reconciliation of the reserve assets, if the value of the reserve assets is in excess of the par value of the approved stablecoins in circulation, the excess amount must be removed from the reserve assets account (client account) within one business day and transferred into the stablecoin issuer's own account.

Addressing Discrepancies: Shortfall

SIO-6.3.3 Upon daily valuation and reconciliation of the reserve assets, if the value of the reserve assets is less than the par value of the approved stablecoins in circulation, licensee must top up the shortfall amount at the earliest but no later than 1 business day. The stablecoin issuer must top up any identified shortfall from their own liquid resources. The CBB must be immediately notified about the shortfall, its value and the measures taken by the licensee to top up the shortfall.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-6	Reserve Asset & Redemption Right

SIO-6.4 Custody of Reserve Assets

SIO-6.4.1 Stablecoin issuers must establish, maintain and implement custody policies, procedures and contractual arrangements that ensure at all times that:

(a) the reserve assets are neither encumbered nor pledged as a financial collateral arrangement;
(b) the reserve assets are held either with a third party i.e. a bank or an investment firm or with an independent custodian;
(c) the stablecoin issuer have prompt access to the reserve assets to meet any requests for redemption from the clients of approved stablecoins;
(d) concentrations of the custodians of reserve assets are avoided;
(e) risk of concentration of reserve assets is avoided.

SIO-6.4.2 The custody policies and procedures referred to in Paragraph SIO-6.4.1 must set out the selection criteria for the appointment of banks, investment firms and independent custodian to safeguard the reserve assets and the procedure for reviewing such appointment. Stablecoin issuers must review the appointment of banks, investment firms, and independent custodians for safeguarding the reserve assets on an annual basis or more frequently. For the purpose of review stablecoin issuers must evaluate their exposures to the banks, investment firms and independent custodians , taking into account the full scope of their relationship with them, and monitor the financial conditions of such entities on an ongoing basis.

SIO-6.4.3 For the purposes of SIO-6.4.1(b) (safeguarding the reserve assets), a stablecoin issuer can (i) manage the reserve assets by holding them with a bank and an investment firm or (ii) appoint an independent custodian to manage the reserve assets. In either case, the stablecoin issuer is legally responsible for ensuring that the reserve assets are safeguarded appropriately and the stablecoin issuer will be subject to the regulatory requirements that are stipulated for reserve assets.

SIO-6.4.4 Stablecoin issuers who issue two or more approved stablecoins must have a custody policy in place for each pool of reserve assets.

SIO-6.4.5 The reserve assets must be held in custody no later than five business days from the date of issuance of the approved stablecoin.

SIO-6.4.6 Stablecoin issuers must exercise all due skill, care and diligence in the selection, appointment and review of banks, investment firms and independent custodians of the reserve assets.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-6	Reserve Asset & Redemption Right

SIO-6.4 Custody of Reserve Assets (continued)

SIO-6.4.7 Stablecoin issuers must ensure that the banks, investment firm and independent custodians of the reserve assets have the necessary expertise and market reputation to safeguard the reserve assets, taking into account the accounting practices, safekeeping procedures and internal control mechanisms of those entities. The contractual arrangements between the stablecoin issuer and the banks, investment firms and the independent custodians must ensure that the reserve assets held with them are protected against claims of the creditors.

SIO-6.4.8 The appointment of custodians of the reserve assets must be done through a contractual agreement. The contractual agreement must, amongst others, regulate the flow of information necessary to enable the stablecoin issuer and the custodians to perform their functions.

SIO-6.4.9 The appointed custodians must act honestly, fairly, professionally, independently and in the interest of the stablecoin issuer and its clients.

SIO-6.4.10 The appointed custodians must not carry out activities with regard to the stablecoin issuer that might create conflicts of interest between the stablecoin issuer, the clients of the stablecoin issuer and themselves unless all of the following conditions are met:

(a) the custodians have functionally and hierarchically separated the performance of their custody tasks from their potentially conflicting tasks;

(b) the potential conflicts of interest have been properly identified, monitored, managed and disclosed by the stablecoin issuers to their clients, in accordance with Section SIO-5.9.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-6	Reserve Asset & Redemption Right

SIO-6.5 Permanent Right of Redemption

SIO-6.5.1 **Stablecoin issuers must, at all times, ensure that holders of approved stablecoins have a direct legal right to redeem the approved stablecoins for the pegged fiat currency at par value.**

SIO-6.5.2 **Stablecoin issuers must ensure that all legitimate redemption request are processed at par value and completed:**

(a) within one business day; or

(b) if the trading and/or settlement of the reserve assets are subject to significant disruption events beyond the control of the licensee, within one business day of the trading and/or settlement of reserve assets no longer being significantly impacted by such disruption events.

SIO-6.5.3 For the purposes of Paragraph SIO-6.5.2, a redemption request is generally deemed as legitimate if the client can meet the stablecoin issuers onboarding requirements, including the applicable customer onboarding rules to mitigate ML/TF risks.

SIO-6.5.4 **Where a stablecoin issuer imposes any type of fees or charges, whether directly or indirectly, on redemption, such fees or charges must be reasonable and must not be set at a very high level to deter the clients from exercising their right to redemption. Stablecoin issuers must clearly communicate the fees and charges on redemption.**

SIO-6.5.5 **Stablecoin issuers must establish, maintain and implement clear and detailed policies and procedures for redemption. The redemption policy and procedure must be disclosed on the stablecoin issuer's website.**

SIO-6.5.6 **Stablecoin issuers must prominently state the conditions and procedures for redemption in the stablecoin whitepaper and on the stablecoin issuer's website. Any condition that the stablecoin issuer wishes to impose for redemption must be reasonable.**

SIO-6.5.7 **Where a stablecoin issuers retain any approved stablecoin for re-circulation following redemption, the retention must be done in accordance with the requirements stipulated Paragraph SIO-5.1.6 i.e. the stablecoin issuer must ensure that the retained approved stablecoins are fully backed by reserve assets.**

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-6	Reserve Asset & Redemption Right

SIO-6.6 Prohibition on Paying Interest

SIO-6.6.1 Stablecoin issuers must not grant any interest, or otherwise make any payments or benefits, whether directly or indirectly, for the purpose of incentivizing clients to acquire, hold, or otherwise use approved stablecoins.

SIO-6.6.2 For the purposes of Paragraph SIO-6.6.1, the following shall be treated as interest:

(a) any remuneration or any other benefit related to the length of time during which a client holds the approved stablecoins;

(b) net compensation or discounts, with the purported effect equivalent or similar to that of interest accrued to a client holding the approved stablecoins, directly from the licensed stablecoin issuer or from third parties, and directly associated to the approved stablecoin or from the remuneration or pricing of other products;

(c) any other benefits (whether or not monetary in nature) which may incentivize clients to acquire, hold, or otherwise use an approved stablecoins, as may be determined by CBB in its absolute discretion.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-7	Stablecoin Whitepaper Requirements

SIO-7.1 Content of Stablecoin Whitepaper

SIO-7.1.1 The draft stablecoin whitepaper referred to in Paragraph SIO-2.1.4(j) must be prepared in accordance with the template provided in Appendix C, either in Arabic or English language, containing all the information concerning the stablecoin issuer and the proposed stablecoin offering that would enable clients to make an informed decision and understand the risks relating to the stablecoin. The information in the draft stablecoin whitepaper must, at a minimum, include the following:

(a) information about the stablecoin issuers;
(b) information about the approved stablecoin;
(c) information about the offering of approved stablecoin to the public and/or its admission to trading;
(d) information on the rights and obligations attached to the approved stablecoin;
(e) information on the underlying technology;
(f) information on the risks;
(g) information on the reserve assets;

SIO-7.1.2 All information in the draft stablecoin whitepaper must be fair, clear and not misleading. The draft stablecoin whitepaper must not contain material omissions and must be presented in a concise and comprehensible form.

Summary of Draft Stablecoin Whitepaper

SIO-7.1.3 Along with the stablecoin whitepaper, a summary of the stablecoin whitepaper, in Arabic and English languages, must be made available to clients. The summary must be in non-technical language, easily understandable, laid out in a clear and comprehensive format and include key information about the stablecoin including the permanent right of redemption at any time and at par value as well as the fees and charges, if any, for such redemption. The summary must also include a warning that:

(a) it should be read as an introduction to the full stablecoin whitepaper; and
(b) clients should base their decision to purchase the approved stablecoin on the content of the stablecoin whitepaper as a whole and not on the summary alone.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-7	Stablecoin Whitepaper Requirements

SIO-7.1 Content of Stablecoin Whitepaper (continued)

Responsibility for Reliability and Accuracy of the Stablecoin Whitepaper

SIO-7.1.4 The stablecoin whitepaper and the modified stablecoin whitepaper must include a duly signed Board of Directors responsibility statement. The signature on the stablecoin whitepaper and the modified stablecoin whitepaper by the Board of Directors must be preceded by a declaration specifying that, to their knowledge, the information presented in the stablecoin whitepaper corresponds to the facts, that there is no omission liable to make it misleading and that they accept full responsibility for the information contained in the stablecoin whitepaper.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-7	Stablecoin Whitepaper Requirements

SIO-7.2 Modification of Published Stablecoin Whitepaper

SIO-7.2.1 Stablecoin issuers must file a modified stablecoin whitepaper and seek the written approval of the CBB prior to any intended change of their business model likely to have a significant influence on the purchase decision of any clients or prospective clients of approved stablecoin, which occurs after the CBB's approval of the stablecoin whitepaper. Such changes include, amongst others, any material modifications to:

(a) the governance arrangements and risk management framework;
(b) the reserve assets and the custody of the reserve assets;
(c) the rights granted to the holders of approved stablecoins;
(d) the mechanism through which the approved stablecoin is issued and redeemed;
(e) the protocols for validating the transactions in approved stablecoins;
(f) the functioning of stablecoin issuer's proprietary distributed ledger technology; where the approved stablecoins are issued, transferred and stored using such a distributed ledger technology;
(g) the mechanisms to ensure the liquidity of approved stablecoins, including the liquidity management policy and procedures;
(h) the arrangements with third-party entities, including for managing the reserve assets and the custody of reserve assets;
(i) the complaints-handling procedures;
(j) the money laundering and terrorist financing risk assessment and general policies and procedures.

SIO-7.2.2 The CBB shall examine the proposed modification to the stablecoin whitepaper and may request additional information, explanation or justification concerning the proposed modification. Where the CBB makes such a request, the stablecoin issuer must provide the additional information requested within 15 days from the date of the request.

SIO-7.2.3 A modified stablecoin whitepaper must comply with the following requirements:

(a) The order of the information appearing in the modified stablecoin whitepaper must be consistent with that of the original stablecoin whitepaper;
(b) Clear identification of the items/paragraphs modified or replaced;
(c) A statement that it is to be read in conjunction with the original stablecoin whitepaper; and
(d) A responsibility statement from the Board of Directors of the licensee.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-7	Stablecoin Whitepaper Requirements

SIO-7.2 Modification of Published Stablecoin Whitepaper (continued)

SIO-7.2.4 Where the CBB approves the modified stablecoin whitepaper, the stablecoin issuer must:

(a) Immediately publish the modified stablecoin whitepaper on its website;

(b) put in place necessary mechanisms to ensure protection of clients, when a modification of the stablecoin issuer's operations can have a material effect on the value, stability, or risks of the approved stablecoins or the reserve assets;

(c) take appropriate corrective measures to address concerns related to market integrity, financial stability or the smooth operation of payment systems.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-7	Stablecoin Whitepaper Requirements

SIO-7.3 Publication of the Stablecoin Whitepaper and Modified Stablecoin Whitepaper

SIO-7.3.1 Stablecoin issuers must publish on their website the approved stablecoins whitepaper referred to in Section SIO-7.1 and, where applicable, the modified stablecoin whitepaper referred to in Section SIO-7.2. The approved stablecoin whitepaper must be publicly accessible at least from the starting date of the offer to the public. The approved stablecoin whitepaper and, where applicable, the modified stablecoin whitepaper must remain available on the stablecoin issuer's website for as long as the approved stablecoins are held by the public.

MODULE	SIO: Stablecoin Issuance & Offering
CHAPTER	SIO-8 Restriction on Issuance, Significant Stablecoin Arrangements & Reporting

SIO-8.1 Restriction on the Issuance of Approved Stablecoins

SIO-8.1.1 **A stablecoin issuer must stop issuing an approved stablecoin when the estimated use of that approved stablecoin, as a medium of exchange within Bahrain (as a means of payment for the provision of goods and services), averaged over immediately preceding quarter:**

(a) exceeds 100,000 transactions per day; and

(b) the per day value of transactions equivalent in BHD exceeds 2,500,000.

The aforementioned restriction on issuance does not apply to approved stablecoins backed by Bahraini Dinar (BHD) or US Dollar (USD).

SIO-8.1.2 For the purposes of SIO-8.1.1;

(a) "transaction" as referred to in SIO-8.1.1(a) means any change of the natural or legal person entitled to the approved stablecoin as a result of the transfer of the approved stablecoin on the distributed ledger (on chain) address or account to another but does not include;

(i) the transfers between different addresses or accounts of the same client;

(ii) when the payer and payee, both, are located outside of Bahrain. For avoidance of doubt, to be considered as a transaction, either the payer or the payee or both must be based out of Bahrain;

(b) "medium of exchange" means the use of approved stablecoin to pay for goods and services within Bahrain, irrespective of whether the payment is made to a merchant or any other payee (natural or legal person). This excludes the exchange approved stablecoin for fiat currency with the stablecoin issuer or with a crypto-asset licensee, unless the approved stablecoin is used for the settlement of transactions in other cryptoassets.

SIO-8.1.3 **A stablecoin issuer must, within 30 days of reaching the thresholds stipulated in Paragraph SIO-8.1.1, submit a plan to the CBB for approval, specifying the measures that the licensee intends to implement to keep the quarterly average number of transactions per day and quarter average value of transaction per day below the stipulated threshold.**

SIO-8.1.4 The CBB shall assess the plan and, where deemed necessary, may modify the plan in order to ensure a timely decrease of the use of the non BHD denominated approved stablecoin as a medium of exchange.

SIO-8.1.5 **Where several stablecoin issuers have issued the approved stablecoins backed by the same fiat currency, the requirement of Paragraph SIO-8.1.1 shall be assessed by the CBB after aggregating the data from all the licensees.**

SIO-8.1.6 **A stablecoin issuer, following suspension of issuance of an approved stablecoin, may again seek the CBB's approval for resumption of issuance of the approved stablecoin provided the licensee is able to demonstrate to the CBB that reissuance of the non BHD denominated approved stablecoin shall not contravene the requirement of Paragraph SIO-8.1.1**

MODULE	SIO: Stablecoin Issuance & Offering
CHAPTER	SIO-8 Restriction on Issuance, Significant Stablecoin Arrangements & Reporting

SIO-8.2 Significant Stablecoins

SIO-8.2.1 The CBB may classify an approved stablecoin as significant stablecoin where the CBB determines that any disruption to the approved stablecoin arrangement could lead to further disruption to its users, cause systemic disruption to the financial system of Bahrain or affect public confidence in the financial system of Bahrain.

SIO-8.2.2 To be classified as a significant stablecoin, an approved stablecoin must meet 3 or more of the following criteria:

(a) the number of clients holding the approved stablecoin is more than 1,000,000;

(b) the par value of the approved stablecoin outstanding, its market capitalisation or the size of the reserve assets backing the approved stablecoin is higher than 5,000,000 BHD;

(c) the per day number and aggregate value of transactions in the approved stablecoin averaged over preceding three months period, is higher than 200,000 transactions and 5,000,000 BHD respectively;

(d) the significance of the activities of the licensee on an international scale, including the use of the approved stablecoins for payments and remittances;

(e) the interconnectedness and interdependency of the of the approved stablecoin or the stablecoin issuer with the wider financial system;

(f) whether the stablecoin issuer has issued more than one approved stablecoin; and

(g) the business, structural and operational complexity of the licensed stablecoin issuer.

SIO-8.2.3 Where the CBB determines that an approved stablecoin meets the requirements of Paragraph SIO-8.2.2 and that the approved stablecoin should be classified as a significant stablecoin, it shall inform the stablecoin issuer about the impending decision, the basis of arriving at the decision and give 15 days to the licensee to provide observations and comments. The CBB shall take into consideration the observations and comments of the licensee before arriving at the final decision.

SIO-8.2.4 Where an approved stablecoin has been classified as significant stablecoin, the CBB shall annually or more frequently reassess the classification.

SIO-8.2 Significant Stablecoins (continued)

Additional Obligations for Licensees whose Stablecoins have been Classified as Significant Stablecoins

SIO-8.2.5 **Where an approved stablecoin is classified as significant stablecoin, the stablecoin issuer issuing such significant stablecoin must:**

(a) adopt, implement and maintain a remuneration policy that promotes the sound and effective risk management and that does not create incentives to relax risk standards;

(b) assess and monitor the liquidity needs to meet the redemption request. For this purpose, the licensee must establish, maintain and implement a liquidity management policy and procedures. The policy and those procedures must ensure that the reserve assets have a resilient liquidity profile that enables the licensee to continue operating normally, including under scenarios of liquidity stress;

(c) conduct, on a regular basis, liquidity stress testing. Depending on the outcome of such tests, the licensee may decide to strengthen the liquidity requirements.

SIO-8.2.6 **Where several stablecoin issuers have issued significant stablecoins backed by same fiat currency, provisions of Paragraph SIO-8.2.5 shall apply to each licensee.**

SIO-8.2.7 The CBB may, in its absolute discretion, impose additional requirements on stablecoin issuer whose approved stablecoin have been classified as significant stablecoin.

MODULE	SIO: Stablecoin Issuance & Offering
CHAPTER	SIO-8 Restriction on Issuance, Significant Stablecoin Arrangements & Reporting

SIO-8.3 Reporting

SIO-8.3.1 **For each approved stablecoin, the stablecoin issuer must on quarterly basis report to the CBB the following information:**

(a) the number of clients holding the approved stablecoin;

(b) the par value of the approved stablecoin issued and the size of the reserve assets;

(c) the average number and average aggregate value of transaction per day during the relevant quarter;

(d) an estimate of the average number and average aggregate value of transaction per day during the quarter that are associated to its use as a medium of exchange within Bharain.

SIO-8.3.2 For the purpose of SIO-8.3.1(c) and SIO-8.3.1(d), "transaction" means any change of the natural or legal person entitled to the approved stablecoin as a result of transfer of the approved stablecoin from on the distributed ledger (on chain) address or account to another but excludes (i) the transfers between different addresses or accounts of the same client and (ii) the exchange of approved stablecoin for fiat currency with the stablecoin issuer or with a crypto-asset licensee, unless the approved stablecoin is used for the settlement of transactions in other crypto-assets and "medium of exchange" means the use of approved stablecoin to pay for goods and services within Bahrain, irrespective of whether the payment is made to a merchant or any other payee (natural or legal person).

SIO-8.3.3 **The information referred to in Paragraph SIO-8.3.1 must be calculated as this information stands on the following reporting reference dates: 31st March, 30th June, 30th September and 31st December and the report must be submitted to the CBB no later than 15 days from the end of the respective reporting period. The value of the transactions referred to in must be reported in Bahraini Dinar by using the relevant exchange rate applicable at the end of each calendar day during the applicable reporting period.**

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-9	Technology Governance & Cyber Security

SIO-9.1 General Requirements

SIO-9.1.1 Stablecoin issuers 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).

SIO-9.1.2 Stablecoin issuers must, as a minimum, have in place systems and controls with respect to the following:

(a) Wallets: Procedures describing the creation, management and controls of 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 approved stablecoins: Systems and controls to mitigate the risk of misuse of approved stablecoins, setting out how:

i. The origin of approved stablecoin is determined, in case of an incoming transaction; and

ii. The destination of approved stablecoin is determined, in case of an outgoing transaction.

SIO-9.1 General Requirements (continued)

(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; and
  iv. Risk of financial crime

SIO-9.1.3 The CBB may grant waiver from specific requirements of technology governance and cyber security. A stablecoin issuer seeking waiver from specific requirements must provide in writing, to the satisfaction of the CBB, that the nature, scale and complexity of their business does not require such technology governance and cyber security measures and in absence of such measures there will be no risk of violation of applicable laws, including the CBB law, its regulations, resolutions or directives (including these rules) or risks associated with the integrity of the market and/or interest of clients.

System Resilience

SIO-9.1.4 Stablecoin issuers must have in place effective systems, procedures and arrangements to ensure that their IT systems are resilient to meet the business requirements.

SIO-9.1.5 Stablecoin issuers must continuously monitor the utilisation of their system resources against a set of pre-defined thresholds. Such monitoring must facilitate the licensee in carrying out capacity management to ensure IT resources are adequate to meet current and future business needs.

SIO-9.1.6 Stablecoin issuers must conduct regular testing of resilience of its IT systems to meet its business requirements.

SIO-9.1.7 A stablecoin issuer's IT systems must be designed and implemented in a manner to achieve the level of system availability that is commensurate with its business needs. Fault-tolerant solutions must be implemented for IT systems which require high system availability and technical glitches must be minimized.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-9	Technology Governance & Cyber Security

SIO-9.2 Maintenance and Development of Systems

SIO-9.2.1 Stablecoin issuers must have a clear and well-structured approach for the implementation and upgrade of systems and software.

SIO-9.2.2 Stablecoin issuers must also have well-established policies and procedures for the regular and thorough testing of any system currently implemented or being considered for use. Stablecoin issuers must ensure that the implementation of new systems, or upgrading of existing systems, is thoroughly checked by multiple members of technology staff.

SIO-9.2.3 Licensed stablecoin issuers must maintain a clear and comprehensive audit trail for system issues internally, including security issues and those with third parties, and their resolution.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-9	Technology Governance & Cyber Security

SIO-9.3 Security Measures and Procedures

SIO-9.3.1 Stablecoin issuers 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.

SIO-9.3.2 The IT infrastructures must provide strong layered security and ensure elimination of "single points of failure". Stablecoin issuers 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.

SIO-9.3.4 Stablecoin issuers 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.

SIO-9.3.5 Stablecoin issuers must have in place policies and procedures that address information security for all staff, sets the security tone for the whole entity and informs staff what is expected of them. All staff should be aware of the sensitivity of data and their responsibilities for protecting it.

SIO-9.3.6 The encryption of data, both at rest and in transit, including consideration of API security should be included in the security policy. In particular, encryption and decryption of 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.

SIO-9.3.7 Stablecoin issuers must conduct regular security tests of their systems, network, and connections.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-9	Technology Governance & Cyber Security

SIO-9.4 Cryptographic Keys and Wallet Storage

SIO-9.4.1 Stablecoin issuers must implement robust procedures and protective measures to ensure the secure generation, storage, backup and destruction of both public and private keys.

SIO-9.4.2 Stablecoin issuers 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.

Private Key Management

SIO-9.4.3 A stablecoin issuer 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 stablecoin issuer using a third party custodian for to hold approved stablecoin must ensure that the third-party custodian establishes and implements such controls and procedures. The procedure must include the following:

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

(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 approved stablecoins 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).

SIO-9.4 Cryptographic Keys and Wallet Storage (continued)

(e) Distributed backups should be stored in a manner that ensures seed and private key cannot be regenerated based solely on the backups stored in the same physical location. Access control to the backups must be as stringent as access control to the original seed and private key.

MODULE	SIO: Stablecoin Issuance & Offering
CHAPTER	SIO-9 Technology Governance & Cyber Security

SIO-9.5 Origin and Destination of Approved Stablecoins

SIO-9.5.1 Stablecoin issuers must consider using technology solutions and other systems to adequately meet anti-money laundering, financial crime and know-your-customer requirements.

SIO-9.5.2 Stablecoin issuers must develop, implement and maintain effective transaction monitoring systems to determine the origin of an approved stablecoin, to monitor its destination and to apply strong "know your transaction" measures which enable the licensed stablecoin issuer to have complete granular data centric information about the transactions conducted by a client.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO- 9	Technology Governance & Cyber Security

SIO-9.6 Planned and Unplanned System Outages

SIO-9.6.1 **Stablecoin issuers must have multiple communication channels to ensure that their clients are informed, ahead of time, of any outages which may affect them.**

SIO-9.6.2 **Stablecoin issuers must have clear, publicly available, procedures articulating the process in the event of an unplanned outage. During an unplanned outage, licensed stablecoin issuers must be able to rapidly disseminate key information and updates on a frequent basis.**

SIO-9.6.3 Stablecoin issuers should have a programme of planned systems outages to provide for adequate opportunities to perform updates and testing.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-9	Technology Governance & Cyber Security

SIO-9.7 Cyber Security

General Requirements

SIO-9.7.1 Stablecoin issuers must establish and maintain an effective cyber security program to ensure the availability and functionality of the licensee's electronic systems and to protect those systems and any sensitive data stored on those systems from unauthorized access, use, or tampering. The cyber security program must be designed to perform, at the minimum, the following five core cyber security functions:

(a) identify internal and external cyber security risks by, at a minimum, identifying the information stored on the licensee's systems, the sensitivity of such information, and how and by whom such information may be accessed;

(b) protect the licensee's electronic systems, and the information stored on those systems, from unauthorized access, use, or other malicious acts through the use of defensive infrastructure and the implementation of policies and procedures;

(c) detect system intrusions, data breaches, unauthorized access to systems or information, malware, and other cyber security events;

(d) respond to detected cyber security events to mitigate any negative effects; and

(e) recover from cyber security events and restore normal operations and services.

SIO-9.7.2 Stablecoin issuers must have a robust cyber security risk management framework that encompasses, at a minimum, the following components:

(a) Cyber security strategy;

(b) Cyber security policy; and

(c) Cyber security risk management approach, tools and methodology and, an organization-wide security awareness program.

SIO-9.7.3 The cyber security risk management framework must be developed in accordance with the National Institute of Standards and Technology (NIST) Cyber security framework which is summarized in Appendix A – Cyber security Control Guidelines. Broadly, the cyber security risk management framework should be consistent with the licensed stablecoin issuer's risk management framework.

SIO-9.7 Cyber Security (continued)

SIO-9.7.4 Senior management, and where appropriate, the boards, should receive comprehensive reports, covering cyber security issues such as the following:

(a) Key Risk Indicators/ Key Performance Indicators;
(b) Status reports on overall cyber security control maturity levels;
(c) Status of staff Information Security awareness;
(d) Updates on latest internal or relevant external cyber security incidents; and
(e) Results from penetration testing exercises.

SIO-9.7.5 Stablecoin issuers may establish a cyber security committee that is headed by an independent senior manager from a control function (like CRO), with appropriate authority to approve policies and frameworks needed to implement the cyber security strategy, and act as a governance committee for the cyber security function. Membership of this committee should include senior management members from business functions, IT, Risk and Compliance.

Roles and Responsibilities of the Board

SIO-9.7.6 The board must provide oversight and accord sufficient priority and resources to manage cyber security risk, as part of the stablecoin issuer's overall risk management framework.

SIO-9.7.7 In discharging its oversight functions, the board must:

(a) Ensure that the licensed stablecoin issuer's strategy, policy and risk management approach relating to cyber security are presented for the board's deliberation and approval;
(b) Ensure that the approved cyber security risk policies and procedures are implemented by the management;
(c) Monitor the effectiveness of the implementation of the stablecoin issuer's cyber security risk policies and procedures and ensure that such policies and procedures are periodically reviewed, improved and updated, where required. This may include setting performance metrics or indicators, as appropriate, to assess the effectiveness of the implementation of cyber security risk policies and procedures;
(d) Ensure that adequate resources are allocated to manage cyber security including appointing a qualified person as Chief Information Security Officer ("CISO") with appropriate authority to implement the cyber security strategy. The CISO is the person responsible and accountable for the effective management of cyber security;
(e) Ensure that the impact of cyber security risk is adequately assessed when undertaking new activities, including but not limited to any new products, investment decision, merger and acquisition, adoption of new technology and outsourcing arrangements;

SIO-9.7 Cyber Security (continued)

(f) Ensure that the management continues to promote awareness on cyber resilience at all levels within the licensee;
(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 licensed stablecoin issuer.

Roles and Responsibilities of the Management

SIO-9.7.8 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 stablecoin issuer. These policies and procedures must take into account the following:
  i. The sensitivity and confidentiality of data which the stablecoin issuer maintains;
  ii. Vulnerabilities of the stablecoin issuer's information systems and operating environment across the licensee; and
  iii. The existing and emerging cyber security threats.
(b) Ensuring that employees, agents (where relevant) and third party service providers are aware and understand the cyber security risk policies and procedures, the possible impact of various cyber security threats and their respective roles in managing such threats;
(c) Recommending to the board on appropriate strategies and measures to manage cyber security risk, including making necessary changes to existing policies and procedures, as appropriate; and
(d) Reporting to the board of any cyber security breaches and periodically update the board on emerging cyber security threats and their potential impact on the stablecoin issuer.

SIO-9.7.9 Management must ensure that:
(a) The stablecoin issuer has identified clear internal ownership and classification for all information assets and data;
(b) The stablecoin issuer has maintained an inventory of the information assets and data which is reviewed and updated regularly;
(c) Employees responsible for cyber security are adequate to manage the licensed stablecoin issuer's cyber security risks and facilitate the performance and continuous improvement of all relevant cyber security controls; and

SIO-9.7 Cyber Security (continued)

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

SIO-9.7.10 With respect to Paragraph SIO-9.7.9(a), data classification entails analyzing the data the stablecoin issuer retains, determining its importance and value, and then assigning it to a category. When classifying data, the following aspects should be determined:

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

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

Cyber Security Strategy

SIO-9.7.11 An organisation-wide cyber security strategy must be defined and documented to include:

(a) The position and importance of cyber security at the stablecoin issuer;
(b) The primary cyber security threats and challenges facing the stablecoin issuer;
(c) The stablecoin issuer's approach to cyber security risk management;
(d) The key elements of the cyber security strategy including objectives, principles of operation and implementation approach;
(e) Scope of risk identification and assessment, which must include the dependencies on third party service providers;
(f) Approach to planning response and recovery activities; and
(g) Approach to communication with internal and external stakeholders, including sharing of information on identified threats and other intelligence among industry participants.

SIO-9.7.12 The cyber security strategy should be communicated to the relevant stakeholders, and it should be revised as necessary and, at least, once every three years. Appendix A provides cyber security control guidelines that can be used as a reference to support the stablecoin issuer's cyber security strategy and cyber security policy.

SIO-9.7 Cyber Security (continued)

SIO-9.7.13 Stablecoin issuer's must implement a written cyber security risk policy setting out the licensee's Board approved policies and related procedures that are approved by senior management, for the protection of its electronic systems and client data stored on those systems. This policy must be reviewed and approved by the licensee's board of directors at least annually. The cyber security policy, among others, must address the following areas:

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

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

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

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

(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 licensed stablecoin issuer's cyber security risk policy;

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

(g) Other key elements of the information security and cyber security risk management including the following:

i. information security;
ii. data governance and classification;
iii. access controls;
iv. business continuity and disaster recovery planning and resources;
v. capacity and performance planning;

SIO-9.7 Cyber Security (continued)

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.

Prevention

SIO-9.7.14 Stablecoin issuers 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.

SIO-9.7.15 The assessment of the vulnerabilities of the stablecoin issuer'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.

SIO-9.7.16 Stablecoin issuers must develop and implement preventive measures to minimise the licensee's exposure to cyber security risk.

SIO-9.7.17 Preventive measures referred to in Paragraph SIO-9.7.16 above must include, at a minimum, the following:
(a) Deployment of End Point Protection (EPP) and End Point Detection and Response (EDR) including anti-virus software and malware programs to detect, prevent and isolate malicious code;
(b) Layering systems and systems components;
(c) Use of firewalls for network segmentation including use of Web Application Firewalls (WAF), where relevant, for filtering and monitoring HTTP traffic between a web application and the Internet, and access control lists to limit unauthorized system access between network segments;

SIO-9.7 Cyber Security (continued)

(d) Rigorous testing at software development stage as well as after deployment to limit the number of vulnerabilities;
(e) Penetration testing of existing systems and networks;
(f) Use of authority matrix to limit privileged internal or external access rights to systems and data;
(g) Use of a secure email gateway to limit email based cyber attacks such as malware attachments, malicious links, and phishing scams (for example use of Microsoft Office 365 Advanced Threat Protection tools for emails);
(h) Use of a Secure Web Gateway to limit browser based cyberattacks, malicious websites and enforce organization policies;
(i) Creating a list of whitelisted applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on the organization's systems; and
(j) Implementing Bring Your Own Device "BYOD" security policies to secure all mobile devices with any access to licensee systems, applications, and networks through security measures such as encryption, remote wipe capabilities, and password enforcement.

SIO-9.7.18 Stablecoin issuers should also implement the following prevention controls in the following areas:
(a) Data leakage prevention to detect and prevent confidential data from leaving the licensee's technology environment;
(b) Controls to secure physical network ports against connection to computers which are unauthorised to connect to the licensee's network or which do not meet the minimum-security requirements defined for licensee computer systems (e.g. Network access control); and
(c) Identity and access management controls to limit the exploitation and monitor the use of privileged and non-privileged accounts.

SIO-9.7.19 Stablecoin issuers must set up anti-spam and anti-spoofing measures to authenticate the licensee's mail server and to prove to ISPs, mail services and other receiving mail servers that senders are truly authorized to send the email. Examples of such measures include:
(a) SPF "Sender Policy Framework";
(b) DKIM "Domain Keys Identified Mail"; and
(c) DMARC "Domain-based Message Authentication, Reporting and Conformance".

SIO-9.7.20 Stablecoin issuers should subscribe to one of the Cyber Threat Intelligence services in order to stay abreast of emerging cyber threats, cybercrime actors and state of the art tools and security measures.

SIO-9.7 Cyber Security (continued)

SIO-9.7.21 **Stablecoin issuers must use a single unified private email domain or its subdomains for communication with clients to prevent abuse by third parties. Stablecoin issuers must not utilise third-party email provider domains for communication with clients. The email domains must comply with the requirements with respect to SPF, DKIM and DMARC in this Module.**

SIO-9.7.22 For the purpose of Paragraph SIO- 9.7.21, stablecoin issuers with subsidiaries or branches outside Bahrain will be allowed to use additional domains subject to CBB's review. Licensees may be allowed, subject to CBB's review, for their clients to receive emails from third-party service providers for specific services offered by such third parties provided the clients were informed and agreed on such an arrangement. Examples of such third-party services include informational subscription services and document management services.

SIO-9.7.23 **Stablecoin issuers must comply with the following requirements with respect to URLs or other clickable links in communications with clients:**

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

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

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

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

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

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

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

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

SIO-9.7 Cyber Security (continued)

Cyber Risk Identification and Assessments

SIO-9.7.24 **Stablecoin issuers must conduct periodic assessments of cyber threats. For the purpose of analysing and assessing current cyber threats relevant to the licensee, it should take into account the factors detailed below:**

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

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

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

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

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

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

SIO-9.7.25 **Stablecoin issuers must conduct periodic assessments of the maturity, coverage, and effectiveness of all cyber security controls. Cyber security control assessment must include an analysis of the controls' effectiveness in reducing the likelihood and probability of a successful attack.**

SIO-9.7.26 Stablecoin issuers should ensure that the periodic assessments of cyber threats and cyber security controls cover all critical technology systems. A risk treatment plan should be developed for all residual risks which are considered to be above the licensee's risk tolerance levels.

SIO-9.7.27 **Stablecoin issuers must conduct regular technical assessments to identify potential security vulnerabilities for systems, applications, and network devices. The vulnerability assessments must be comprehensive and cover internal technology, external technology, and connections with third parties. Preferably, monthly assessments should be conducted for internal technology and weekly or more frequent assessments for external public facing services and systems.**

SIO-9.7.28 With respect to Paragraph SIO-9.7.27, external technology refers to the stablecoin issuer's public facing technology such as websites, apps and external servers. Connections with third parties includes any API or other connections with fintech companies, technology providers, outsourcing service providers etc.

SIO-9.7 Cyber Security (continued)

SIO-9.7.29 Stablecoin issuers must have in place vulnerability and patch management processes which include remediation processes to ensure that the vulnerabilities identified are addressed and that security patches are applied where relevant within a timeframe that is commensurate with the risks posed by each vulnerability.

SIO-9.7.30 Stablecoin issuers must perform vulnerability assessment and penetration testing of their systems, applications, and network devices to verify the robustness of the security controls in place at least twice a year. These tests must be used to simulate real world cyber-attacks on the technology environment and must:

(a) Follow a risk-based approach based on an internationally recognized methodology, such as National Institute of Standards and Technology "NIST" and Open Web Application Security Project "OWASP";
(b) Include both Grey Box and Black Box testing in its scope;
(c) Be conducted by qualified and experienced security professionals who are certified in providing penetration testing services;
(d) Be performed internally at periodic intervals by employees having adequate expertise and competency in such testing;
(e) Be performed, twice a year, by external independent third parties who are rotated out at least every two years; and
(f) Be performed on either the production environment or on nonproduction exact replicas of the production environment.

SIO-9.7.31 The CBB may require additional third party security reviews to be performed as needed.

SIO-9.7.32 The time period between two consecutive penetration test and the vulnerability assessment by an independent third party, referred to in Paragraph SIO-9.7.30(e) must be 6 months and the report on such testing must be provided to CBB within two months following the end of the month where the testing took place. The vulnerability assessment and penetration testing reports must include the vulnerabilities identified and a full list of 'passed' tests and 'failed' tests together with the steps taken to mitigate the risks identified.

Cyber Incident Detection and Management

SIO-9.7.33 Stablecoin issuers must implement cyber security incident management processes to ensure timely detection, response and recovery for cyber security incidents. This includes implementing a monitoring system for log correlation and anomaly detection.

SIO-9.7 Cyber Security (continued)

SIO-9.7.34 Stablecoin issuers should receive data on a real time basis from all relevant systems, applications, and network devices including operational and business systems. The monitoring system should be capable of identifying indicators of cyber incidents and initiate alerts, reports, and response activities based on the defined cyber security incident management process.

SIO-9.7.35 Stablecoin issuers should retain the logs and other information from the monitoring system for detecting cyber incidents, including "low-and-slow" attacks, in order to facilitate incident investigations, for 12 months or longer.

SIO-9.7.36 Once a cyber incident is detected, stablecoin issuers should activate their containment measures, processes and technologies best suited to each type of cyber incident to prevent a cyber incident from inflicting further damage. This may involve, after considering the costs, business impact and operational risks, shutting down or isolating all or affected parts of their systems and networks as deemed necessary for containment and diagnosis.

SIO-9.7.37 Stablecoin issuers must define roles and responsibilities and assign adequate resources to detect, identify, investigate and respond to cyber incidents that could impact the licensee's infrastructure, services and clients. Such responsibilities must include log correlation, anomaly detection and maintaining the licensee's asset inventory and network diagrams.

SIO-9.7.38 Stablecoin issuers must regularly identify, test, review and update current cyber security risk scenarios and the corresponding response plan. This is to ensure that the scenarios and response plan remain relevant and effective, taking into account changes in the operating environment, systems or the emergence of new cyber security threats. If any gaps are identified, the monitoring system must be updated with new use cases and rule sets which are capable of detecting the current cyber incident scenarios.

SIO-9.7.39 The cyber incident scenario tests should include high-impact-low-probability events and scenarios that may result in failure. Common cyber incident scenarios include distributed denial of service (DDoS) attacks, system intrusion, data exfiltration and system disruption. Stablecoin issuers should regularly use threat intelligence to update the scenarios so that they remain current and relevant. Stablecoin issuers should periodically review current cyber incident scenarios for the purpose of assessing the licensee's ability to detect and respond to these scenarios if they were to occur.

SIO-9.7 Cyber Security (continued)

SIO-9.7.40 **Stablecoin issuers must ensure that critical cyber security incidents detected are escalated to an incident response team, management and the Board, in accordance with the licensee's business continuity plan and crisis management plan, and that an appropriate response is implemented promptly. Also refer to Paragraph SIO-9.7.61 for the requirement to report to the CBB.**

SIO-9.7.41 Stablecoin issuers should clearly define the roles, responsibilities and accountabilities for cyber incident detection and response activities to one or more named individuals that meet the pre-requisite role requirements. Potential conflicts of interest are minimised by ensuring a separation of implementation and oversight roles where possible. The roles should include:

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

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

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

SIO-9.7.42 For the purpose of managing a critical cyber incident, stablecoin issuers should operate a situation room, and should include in the incident management procedure a definition of the authorities and responsibilities of staff members, internal and external reporting lines, communication channels, tools and detailed working procedures. The situation room or a war room is a physical room or a virtual room where relevant members of the management gather to handle a crisis in the most efficient manner possible.

SIO-9.7.43 Stablecoin issuers should record and document in an orderly manner the incidents that have been handled and the actions that were taken by the relevant functions. In particular, a licensed stablecoin issuer should maintain an "incident log" in which all the notifications, decisions and actions taken, in relation to cyber incidents, are documented, as close as possible to the time of their occurrence. It should also include the status of the issue whether it is open or has been resolved and the person in charge of resolving the issue/incident. The logs should be stored and preserved in a secure and legally admissible manner.

SIO-9.7 Cyber Security (continued)

SIO-9.7.44 Stablecoin issuers should utilise pre-defined taxonomy for classifying cyber incidents according to, for example, the type of incident, threat actors, threat vectors and repercussions; and a pre-established severity assessment framework to help gauge the severity of the cyber incident. For example, taxonomies that can be used when describing cyber incidents:

(a) Describe the cause of the cyber incident (e.g. process failure, system failure, human error, external event, malicious action).
(b) Describe whether the cyber incident is due to a third-party service provider.
(c) Describe the attack vector (e.g. malware, virus, worm, malicious hyperlink).
(d) Describe the delivery channel used (e.g. e-mail, web browser, removable storage media).
(e) Describe the impact (e.g. service degradation/disruption, service downtime, potential impact to clients, data leakage, unavailability of data, data destruction/corruption, reputational damage).
(f) Describe the type of incident (e.g. zero-day attack, exploiting a known vulnerability, isolated incident).
(g) Describe the intent (e.g. malicious, theft, monetary gain, fraud, political, espionage, opportunistic).
(h) Describe the threat actor (e.g. script kiddies, amateur, criminal syndicate, hacktivist, nation state).
(i) The cyber incident severity may be classified as:
(a) **Severity 1** incident has caused or will cause a serious disruption or degradation of critical service(s) and there is potentially high impact on public confidence in the stablecoin issuer.
(b) **Severity 2** incident has or will cause some degradation of critical services and there is medium impact on public confidence in the licensee.
(c) **Severity 3** incident has little or no impact to critical services and there is no visible impact on public confidence in the stablecoin issuer.

SIO-9.7.45 Stablecoin issuers should determine the effects of the cyber incident on clients and to the wider financial system as a whole and report the results of such an assessment to the CBB if it is determined that the cyber incident may have a systemic impact.

SIO-9.7.46 Stablecoin issuers should establish metrics to measure the impact of a cyber incident and to report to management the performance of response activities. Examples include:

(a) Metrics to measure impact of a cyber incident:
  i. Duration of unavailability of critical functions and services;
  ii. Number of stolen records or affected accounts;
  iii. Volume of clients impacted;
  iv. Amount of lost revenue due to business downtime, including both existing and future business opportunities; and
  v. Percentage of service level agreements breached.

SIO-9.7 Cyber Security (continued)

(b) Performance metrics for incident management:
   i. Volume of incidents detected and responded via automation;
   ii. Dwell time (i.e. the duration a threat actor has undetected access until completely removed); and
   iii. Recovery Point objectives (RPO) and recovery time objectives (RTO) satisfied.

SIO-9.7.47 **Stablecoin issuers must identify the critical systems and services within its operating environment that must be recovered on a priority basis in order to provide certain minimum levels of service during the downtime and determine how much time the licensee will require to return to full service and operations.**

SIO-9.7.48 Critical incidents are defined as incidents that trigger the BCP and the crisis management plan. Critical systems and services are those whose failure can have material impact on any of the following elements:
(a) Financial situation;
(b) Reputation;
(c) Regulatory, legal and contractual obligations;
(d) Operational aspects; and
(e) Delivery of key products and services.

SIO-9.7.49 **Stablecoin issuers must define a program for recovery activities for the purpose of timely restoration of any capabilities or services that were impaired due to a cyber security incident. Stablecoin issuers must establish recovery time objectives ("RTOs"), i.e. the time within which the intended process is to be covered, and recovery point objectives ("RPOs"), i.e. point to which information used must be restored to enable the activity to operate on resumption. Licensees must also consider the need for communication with third party service providers, clients and other relevant external stakeholders as may be necessary.**

SIO-9.7.50 **Stablecoin issuers must ensure that all critical systems are able to recover from a cyber security breach within the licensee's defined RTO in order to provide important services or some level of minimum services for a temporary period of time.**

SIO-9.7.51 Stablecoin issuers should validate that recovered assets are free of compromise, fully functional and meet the security requirements before returning the systems to normal business operations. This includes performing checks on data to ensure data integrity. In some cases, licensees may need to use backup data kept in a disaster recovery site or plan for the reconstruction of data from external stakeholders such as business partners and clients.

SIO-9.7 Cyber Security (continued)

SIO-9.7.52 **Stablecoin issuers must define a program for exercising the various response mechanisms, taking into account the various types of exercises such as attack simulations, "war games" and "tabletop" exercises, and with reference to the relevant stakeholders such as technical staff, crisis management team, decision-makers and spokespersons.**

SIO-9.7.53 **Stablecoin issuers must define the mechanisms for ensuring accurate, timely and actionable communication of cyber incident response and recovery activities with the internal stakeholders, including to the board or designated committee of the board.**

SIO-9.7.54 **A stablecoin issuer must ensure its business continuity plan is comprehensive and includes a recovery plan for its systems, operations and services arising from a cyber security incident breach.**

Chief Information Security Officer

SIO-9.7.55 **A stablecoin issuer's CISO, as referred to in Paragraph SIO-9.7.7(d), is responsible for overseeing and implementing the stablecoin issuer's cyber security program and enforcing its cyber security policy. The CISO must report to an independent risk management function or the stablecoin issuer must incorporate the responsibilities of cyber security risk into the risk management function.**

Cyber Risk Insurance

SIO-9.7.56 **A stablecoin issuer, based on the assessment of cyber security risk exposure and with an objective to mitigate cyber security risk, must evaluate and consider the option of availing cyber risk insurance. The evaluation process to determine suitability of cyber risk insurance as a risk mitigant must be undertaken on a yearly basis and be documented by the licensee.**

SIO-9.7.57 The cyber risk insurance policy, referred to in Paragraph SIO-9.7.56, may include some or all of the following types of coverage, depending on the risk assessment outcomes:

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

(b) Claim expenses such as costs of defending lawsuits, judgments and settlements, and costs of responding to regulatory investigations;

(c) Coverage for a variety of torts, including invasion of privacy or copyright infringement; and

SIO-9.7 Cyber Security (continued)

(d) Coverages relating to loss of revenue due to interruption of data systems resulting from a cyber or denial of service attack and other costs associated with the loss of data collected by the licensee.

Training and Awareness

SIO-9.7.58 **Stablecoin issuers must evaluate improvement in the level of awareness and preparedness to deal with cyber security risk to ensure the effectiveness of the training programmes implemented.**

SIO-9.7.59 **Stablecoin issuer must ensure that all employees receive adequate training on a regular basis, in relation to cyber security and the threats they could encounter, such as through testing employee reactions to simulated cyber-attack scenarios. All relevant employees must be informed on the current cyber security breaches and threats. Additional training should be provided to 'higher risk staff'.**

SIO-9.7.60 **Stablecoin issuers must ensure that role specific cyber security training is provided on a regular basis to relevant staff including: (a) Executive board and senior management; (b) cyber security roles; (c) IT staff; and (d) any high-risk staff as determined by the stablecoin issuer.**

Reporting to the CBB

SIO-9.7.61 **Upon occurrence or detection of any cyber security incident or detection of any unplanned outages, whether internal or external, that compromises client information or disrupts critical services that affect operations, stablecoin issuers must contact the CBB, immediately (within one hour), on 17547477 and submit Section A of the Cyber Security Incident Report (Appendix-B) to the CBB's cyber incident reporting email, incident.cra@cbb.gov.bh, as soon as possible, but not later than two hours, following occurrence or detection of any cyber incidents.**

SIO-9.7.62 **Following the submission referred to in Paragraph SIO-9.7.61, the stablecoin issuer must submit to the CBB Section B of the Cyber Security Incident Report (Appendix B) within 10 calendar days of the occurrence of the cyber security incident. The stablecoin issuer must include all relevant details in the report, including the full root cause analysis of the cyber security incident, its impact on the business operations and clients, and all measures taken by the stablecoin issuer to stop the attack, mitigate its impact and to ensure that similar events do not recur. In addition, a weekly progress update must be submitted to CBB until the incident is fully resolved**

SIO-9.7 Cyber Security (continued)

SIO-9.7.63 With regards to the submission requirement mentioned in Paragraph SIO-9.7.62, the stablecoin issuer should submit the report with as much information as possible even if all the details have not been obtained yet.

SIO-9.7.64 The vulnerability assessment and penetration testing report (refer Paragraph SIO-9.7.32), along with the steps taken to mitigate the risks must be maintained by the licensee for a five-year period from the date of the report.

SIO-9.8 Cyber Hygiene Practices

Multi Factor Authentication

SIO-9.8.1 Stablecoin issuers must ensure that every client account is secured to prevent any unauthorized access to or use of client account.

SIO-9.8.2 Stablecoin issuers must use multi-factor authentication (two or more factors) to authenticate the identity and authorisation of clients with whom it conducts business. Licensees must, at a minimum, establish adequate security features for client authentication including the use of at least two of the following three elements:

(a) Knowledge (something that only the user knows), such as a pin or password;
(b) Possession (something only the user possesses such as a mobile phone, smart watch, smart card or a token; and
(c) Inherence (something that the user is), such as fingerprint, facial recognition, voice patterns, DNA signature and iris format.

SIO-9.8.3 Stablecoin issuers must ensure that at least one of the factors for authentication referred to in Paragraph SIO-9.8.2 is a dynamic or non-replicable factor unless one of the factors is inherence.

SIO-9.8.4 For the purpose of Paragraph SIO-9.8.2, stablecoin issuers must ensure that the authentication elements are independent from each other, in that the breach of one does not compromise the reliability of the other and are sufficiently complex to prevent forgery.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-10	Custody Arrangements for Approved Stablecoins

SIO-10.1 General Requirements

SIO-10.1.1 This chapter applies to stablecoin issuers who also undertake safeguarding, storing, holding or maintaining custody of approved stablecoins.

SIO-10.1.2 A stablecoin issuer who undertakes safeguarding, storing, holding or maintaining custody of approved stablecoins must have systems and controls in place to:

(a) Ensure the proper safeguarding of approved stablecoins;
(b) Ensure that such safe custody of approved stablecoins is identifiable and secure at all times; and
(c) Ensure protection against the risk of loss, theft or hacking.

SIO-10.1.3 A stablecoin issuer undertaking custody services must hold approved stablecoins of the same type and amount which it holds on behalf of its clients.

SIO-10.1.4 Stablecoin issuers are prohibited from selling, transferring, assigning, lending, hypothecating, pledging, or otherwise using or encumbering approved stablecoins stored, held, or maintained by, or under the custody or control of, such licensee on behalf of a client except for the redemption or transfer of the approved stablecoins at the direction of the client.

Multi-Signature Arrangement

SIO-10.1.5 A stablecoin issuer that maintains custody or control of approved stablecoins must not, at any time, permit arrangements whereby just a party or signatory is able to completely authorise the movement, transfer or withdrawal of approved stablecoins 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 approved stablecoins held under custody by the licensee.

SIO-10.1.6 Stablecoin issuers that maintain custody or control of approved stablecoins are required to mitigate the risk of collusion between the authorised persons or signatories who are able to authorise the movement, transfer or redemption of approved stablecoins held under custody.

SIO-10.1.7 Stablecoin issuers that maintain custody or control of approved stablecoins must 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 approved stablecoins it is holding under custody on behalf for clients have been compromised, such as in the event of a hacking attack, theft or fraud.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-10	Custody Arrangements for Approved Stablecoins

SIO-10.1 General Requirements (continued)

Such policies and procedures must detail the specific steps the licensee will take to protect client's approved stablecoins in the event of such incidents. Licensed stablecoin issuers must also have the ability to immediately halt all further transactions with regard to the approved stablecoin.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-10	Custody Arrangements for Approved Stablecoins

SIO-10.2 Custodial Arrangements

SIO-10.2.1 Stablecoin issuers must provide to the CBB, for prior written approval, details of custodial arrangement put in place to safeguard, store, hold or maintain custody of approved stablecoins.

SIO-10.2.2 Stablecoin issuers may implement the following three types of custodial arrangements or any other type of custodial arrangement that is acceptable to the CBB:

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

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

c) The stablecoin issuer wholly allows clients to "self-custodise" their approved stablecoins. Such an arrangement includes scenarios where licensees require clients to self-custodise their approved stablecoins. Clients are required to source and use their own third party 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 approved stablecoins out of this wallet to another wallet from a third-party wallet provider chosen by the client (and which the licensee does not control).

Third Party Custody Arrangement

SIO-10.2.3 For the purposes of Paragraph SIO-10.2.2(b), where a stablecoin issuer provides a third party custodian to a client it must undertake an appropriate risk assessment of that custodian. Stablecoin issuers must also retain ultimate responsibility for safe custody of approved stablecoins held on behalf of clients and ensure that they continue to meet all their regulatory obligations with respect to custody service and outsourced activities.

SIO-10.2.4 In undertaking an appropriate risk assessment of the third party custodian in accordance with Paragraph SIO-10.2.3, stablecoin issuers should take into account any or all of the following:

(a) The expertise and market reputation of the third party custodian, and once an approved stablecoin has been lodged by the licensee with the third party custodian, the crypto-asset custodian's performance of its services to the licensee;

(b) The arrangements, including cyber security measures, for holding and safeguarding approved stablecoins;

(c) An appropriate legal opinion as to the protection of approved stablecoins in the event of insolvency of the custodian;

(d) Whether the third party custodian is regulated and by whom;

(e) The capital or financial resources of the third party custodian;
(f) The credit rating of the third party custodian; and
(g) Any other activities undertaken by the third party custodian and, if relevant, any affiliated company.

SIO-10.2.5 **When assessing the suitability of the third party custodian, the stablecoin issuers must ensure that the third party custodian will ensure full protections to client assets and that the client assets are fully segregated, both legally and operationally, from the own assets of the third party custodian.**

SIO-10.2.6 **A stablecoin issuer that safeguards, stores, holds or maintains custody of approved stablecoins with a third party custodian, must establish and maintain a system for assessing the appropriateness of its selection of the custodian and assess the continued appointment of that 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 approved stablecoin custodian.**

Self-Custody Arrangement

SIO-10.2.7 **For the purposes of Paragraph SIO-10.2.2(c), the CBB considers scenarios where clients are required to self-custodise their approved stablecoins as being a material risk given that the burden of protecting and safeguarding approved stablecoins falls wholly upon clients. As such, stablecoin issuers requiring clients to self-custodise approved stablecoins are required to disclose this fact fully and clearly upfront to clients.**

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-11	Recovery & Redemption Plan

SIO-11.1 Recovery Plan

SIO-11.1.1 **A stablecoin issuer must draw up and maintain a recovery plan providing for measures to be taken by the stablecoin issuer to restore compliance with the requirements applicable to the reserve assets in cases where the stablecoin issuer fails to comply with those requirements.**

SIO-11.1.2 **The recovery plan referred to in Paragraph SIO-11.1.1 must also include the preservation of the stablecoin issuer's services related to the approved stablecoin, the timely recovery of operations and the fulfilment of the stablecoin issuer's obligations in case of occurrence of events that pose a significant risk leading to disruption of operations.**

SIO-11.1.3 **The recovery plan must include appropriate conditions and procedures to ensure the timely implementation of recovery actions as well as a wide range of recovery options, including:**

(a) liquidity fees on redemptions;

(b) limits on the amount of the approved stablecoin that can be redeemed on any working day;

(c) suspension of redemptions.

SIO-11.1.4 **A stablecoin issuer must submit the draft recovery plan to the CBB for approval, within six months of the date of approval of the stablecoin whitepaper. The CBB may, at its sole discretion, recommend amendments to the draft recovery plan where necessary to ensure its proper implementation. The CBB shall inform the stablecoin issuer about its decision i.e. either approving the draft recovery plan or recommending amendments to the draft recovery plan, within 30 days from the date of submission of the draft recovery plan. The stablecoin issuer must implement the recovery plan as approved by the CBB within 15 days from the date of approval of the recovery plan. The stablecoin issuer must regularly review and update the recovery plan.**

SIO-11.1.5 **Where a stablecoin issuer fails to comply with the requirements applicable to the reserve assets and redemption requirements as referred to in Chapter 6 of this Module or, due to a rapidly deteriorating financial condition, is likely in the near future to not comply with those requirements, the CBB, in order to ensure compliance with the applicable requirements, may, at its sole discretion, require the stablecoin issuer to implement one or more of the arrangements or measures set out in the recovery plan or to update such a recovery plan when the circumstances are different from the assumptions set out in the initial recovery plan and implement one or more of the arrangements or measures set out in the updated plan within a specific timeframe.**

SIO-11.1.6 In the circumstances referred to in Paragraph SIO-11.1.5, the CBB may temporarily suspend the redemption of approved stablecoins, provided that the suspension is justified having regard to the interests of the clients and financial stability.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-11	Recovery & Redemption Plan

SIO-11.2 Content of Recovery Plan

SIO-11.2.1 The recovery plan must include the following:

a) information on governance, including a framework of recovery plan indicators and monitoring thresholds, as specified in Paragraph SIO-11.2.2.

b) The description of the applicable recovery options, including at least a recovery scenario analysis, a description of preparatory measures and information on the preservation of services as specified in Paragraphs SIO-11.2.2 to SIO-11.2.4.

c) The recovery plan's communication and disclosure plan.

Information on Governance

SIO-11.2.2 Stablecoin issuers must include in their recovery plan a clear and detailed description of the governance processes related to the development, maintenance and implementation of the recovery plan.

SIO-11.2.3 For the purposes of Paragraph SIO-11.2.2, the information on governance should cover at a minimum, the following:

(a) the role(s) and function(s) of the person(s) responsible for preparing, implementing and updating the plan;

(b) the description of how the recovery plan fits with the stablecoin issuer's internal governance, business strategy and risk management framework;

(c) the description of the processes and timeframes to be used for the periodical update of the plan and for updating it to respond to any material changes affecting the specific stablecoin, the licensed stablecoin issuer or its environment;

(d) the policies and procedures governing the approval of the recovery plan and its reviews and updates;

(e) the escalation procedures, meaning the conditions and procedures necessary to ensure the timely implementation of particular recovery options foreseen in the recovery plan. It should include clear information on the decision-making process with regard to the activation of the recovery plan based on a detailed escalation process that applies when a breach of a recovery plan indicator threshold is detected or is likely to materialise in the near future, to consider and determine which recovery option may need to be applied to restore the compliance with the relevant regulatory requirements applicable to the reserve asset or to continue rendering services related to the relevant approved stablecoin;

(f) the time limit for the decision on taking recovery actions and the point in time, as well as the modalities, for informing the CBB;

(g) the description of quantitative and qualitative indicators reflecting possible vulnerabilities, weaknesses or threats to the amount, liquidity and allocation of the reserve assets and the funds that stablecoin issuers have to maintain at any time.

SIO-11.2 Content of Recovery Plan (continued)

SIO-11.2.4 **Where stablecoin issuers have entered in an arrangement with third party entities for operating the reserve assets, and for the investment of the reserve assets or for the custody of the reserve assets, they must include in their recovery plan a clear and detailed description of the processes established to exchange information in a way that would ensure the timely activation of the escalation process laid down in Paragraph SIO-11.2.10 in case a breach of recovery plan indicators is detected, either by the stablecoin issuer or by the relevant third party entity. A stablecoin issuer must also specify in the recovery plan how the agreement with any of those third parties ensures the information is timely shared in a way that would allow the stablecoin issuer to be aware of the breach or to acknowledge that the breach is likely to occur in the near future so that the plan can be activated in a timely manner.**

Recovery Plan Indicators & Monitoring Thresholds

SIO-11.2.5 **Stablecoin issuers must lay down in the recovery plan an adequate framework of recovery plan indicators, via which the stablecoin issuer can establish predetermined criteria that may signal the necessity of an increased frequency of monitoring or the activation of the recovery plan. These criteria should be set in a way to allow the stablecoin issuer to monitor, escalate and activate recovery options as appropriate.**

SIO-11.2.6 **Recovery plan indicators must reflect both the approved stablecoin's and the stablecoin issuer's specific risk profile and operating environment. As such, the calibration of recovery plan indicators and thresholds must be applied at the level of the approved stablecoin, except for the capital adequacy indicators that should be calibrated at the level of the stablecoin issuer, based on its specific size, complexity, nature and business model and the operational risk indicators and the market confidence indicators that must be calibrated both at the level of the stablecoin issuer and at the level of the approved stablecoin.**

SIO-11.2.7 When assessing what type of indicators will be included in the recovery plans, a stablecoin issuer should carefully consider the types of events that may lead to a breach of regulatory requirements and elaborate specific indicators based on its internal risk assessment. Therefore, stablecoin issuers should not limit their set of recovery plan indicators to the list provided in Appendix D. Rather, they should consider the list of indicators provided Appendix D as illustrative, so they may choose any or all of the indicators under each category.

SIO-11.2 Content of Recovery Plan (continued)

SIO-11.2.8 Stablecoin issuers must include in the recovery plan that they will monitor the recovery plan indicators with an adequate frequency which would allow the timely submission of the indicators data records to the CBB upon request stablecoin issuers must also specify how they will monitor the said indicators.

SIO-11.2.9 Stablecoin issuers must include recovery plan indicators of both quantitative and qualitative nature. When setting the quantitative recovery plan indicator thresholds, consistently with their overall risk management, stablecoin issuers must use progressive metrics ('traffic light approach') in order to inform the stablecoin issuer's management that such indicators threshold could potentially be reached.

SIO-11.2.10 Stablecoin issuers must ensure that any breach of recovery plan indicator threshold is reported as soon as practicable to the senior management but within a maximum of 24 hours, by activating the appropriate escalation process and, where relevant, acted upon. In addition, any breach of recovery plan indicator threshold and activation of internal escalation matrix must be notified to the CBB within 24hrs following the breach of recovery plan indicator threshold.

SIO-11.2.11 Where a recovery plan indicator has been breached, the stablecoin issuer must assess the situation, decide whether to trigger the activation of the recovery plan and promptly notify the CBB.

Recovery Options

SIO-11.2.12 Stablecoin issuers must include in their recovery plan a range of recovery options that are tailored to the stablecoin issuer's business model and the nature of the approved stablecoin issued.

SIO-11.2.13 The recovery options referred to in Paragraph SIO-11.1.3 and SIO-11.2.12 must include the following:

(a) the recovery plan must set a maximum amount for liquidity fees to be imposed on redemptions;

(b) in setting the maximum amount of liquidity fees to be imposed on redemptions, stablecoin issuers must ensure that this recovery option is not applied as a means to increase the issuer's liquidity resources at the expenses of clients. Stablecoin issuers must ensure that this recovery options are applied only temporarily during the distress phase with the sole purpose to reduce redemption requests while stabilising the value of the approved stablecoin;

SIO-11.2 Content of Recovery Plan (continued)

(c) the recovery plan should set out different quantitative levels of limits on the number or amount of approved stablecoins that can be redeemed on any working day. These levels should be determined based on the severity of the breach(es) of recovery plan indicators and must be set both at aggregate level (e.g. as a percentage of the entire amount of approved stablecoin issued) and at wallet level;

(d) the recovery plan should explain what other remedial actions the stablecoin issuer will take once it has suspended redemptions. Stablecoin issuers must include in their recovery plan that they will consider that suspending redemptions could negatively impact their reputation and the confidence of clients and result in higher volumes of redemption requests once the suspension is lifted. Stablecoin issuers must include in their recovery plan that they will especially consider whether the lift of the suspension should be accompanied by other measures, including but not limited to liquidity fees or limits to the amount of approved stablecoins that can be redeemed on a daily basis;

(e) stablecoin issuers must include in the recovery plan how they plan to restore compliance with the regulatory requirements and clearly communicate to the market the next steps.

SIO-11.2.14 Stablecoin issuers must outline for every recovery option how the continuity of operations will be ensured when implementing that option. This must include an analysis of internal operations (e.g. information technology systems, and human resources operations) and of the access of the stablecoin issuer to key services from third parties which are essential for the regular conduct of its operations.

Continuity of Service

SIO-11.2.15 Stablecoin issuers must include in the recovery plan the mechanism and process they intend to implement to recover operations in a timely manner and fulfil their obligations in case of events that pose a significant risk of disrupting operations. Stablecoin issuers must also include in the recovery plan the services they intend to preserve based on their business model and detail how they will ensure the continuation of the services related to approved stablecoins. The list of services to be continued must at least include services related to the issuance and the redemption of approved stablecoins. Where the implementation of the recovery options has the potential to negatively impact the stablecoin issuer's provision of any of the services identified, the description of the recovery options must outline how the stablecoin issuer plans to ensure the continuity of said services when implementing the recovery plan.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-11	Recovery & Redemption Plan

SIO-11.3 Redemption Plan

SIO-11.3.1 A stablecoin issuer must draw up and maintain an operational plan to support the orderly redemption of each approved stablecoin, which is to be implemented upon a decision by the CBB that the stablecoin issuer is unable or likely to be unable to fulfil its obligations, including in the case of insolvency or in the case of withdrawal of license of the stablecoin issuer.

SIO-11.3.2 The redemption plan must demonstrate the ability of the stablecoin issuer to carry out the redemption of the outstanding approved stablecoins issued without causing undue economic harm to its clients or to the stability of the markets of the reserve assets. The redemption plan must ensure equitable treatment to all the clients and that the clients are paid in a timely manner with the proceeds from the sale of the reserve assets. In addition, the redemption plan must also ensure the continuity of any critical activities that are necessary for the orderly redemption, whether performed by the stablecoin issuer or by any third-party entity.

SIO-11.3.3 A stablecoin issuer must submit the draft redemption plan to the CBB for approval, within six months of the date of approval of the stablecoin whitepaper. The CBB may, at its sole discretion, recommend amendments to the draft redemption plan where necessary to ensure its proper implementation. The CBB shall inform the stablecoin issuer about its decision, i.e. either approving the draft redemption plan or recommending amendments to the draft redemption plan, within 30 days from the date of submission of the draft redemption plan. The stablecoin issuer must implemented the redemption plan as approved by the CBB within 15 days from the date of approval of the redemption plan. The stablecoin issuer must regularly review and update the redemption plan.

General Principles and Objectives of the Redemption Plan

SIO-11.3.4 Where a stablecoin issuer has more than one outstanding issuance of approved stablecoins, the redemption plan of each approved stablecoin must appropriately address the interconnectedness between outstanding approved stablecoins.

SIO-11.3.5 The redemption plan must ensure equitable treatment of all clients holding the approved stablecoin, and the protection of the right of redemption attached to the approved stablecoin as described in the stablecoin whitepaper.

SIO-11.3 Redemption Plan (continued)

SIO-11.3.6 In order to ensure equitable treatment to all clients holding the approved stablecoin, the stablecoin issuer should include in the redemption plan how the individual redemption of claims will be suspended upon the adoption of the CBB's decision triggering the implementation of the redemption plan for the orderly and collective redemption of the approved stablecoin.

SIO-11.3.7 Stablecoin issuers must frame the redemption plan on the assumption that the remaining reserve assets underpinning the relevant approved stablecoin will be used for the benefit of all clients redemption claims when the CBB determines that the stablecoin issuer will not be able to or likely to be unable to fulfil its obligations towards the clients. This must be without prejudice to the right of the clients that the portion of their claim (if any) left unsatisfied by the liquidation of the remaining reserve assets, must be met by the licensed stablecoin issuer in accordance with the applicable law including the applicable insolvency law.

SIO-11.3.8 The redemption plan must ensure that the redemption process does not impose undue economic cost on the clients. Further, the redemption plan must indicate how the costs for the implementation of the redemption plan, such as for the appointment of consultants or intermediaries, or in connection with the liquidation of the reserve of assets will be covered.

SIO-11.3.9 In order to ensure the effectiveness of the right of redemption and that undue economic cost does not affect the clients, the stablecoin issuer must ensure in the redemption plan that the costs for the liquidation of the reserve assets or otherwise linked to the implementation of the redemption plan must only be allocated to the proceeds of the liquidation of the reserve assets after the amount for meeting the relevant clients redemption claims is set aside.

SIO-11.3.10 Costs indicated in the redemption plan should be identified via transparent processes, be reasonable and duly justified.

SIO-11.3.11 The redemption plan must aim to ensure the maximization of the proceeds from the liquidation of the remaining reserve assets within a reasonable timeframe. For this purpose, the stablecoin issuer must develop redemption scenarios under ordinary and stressed market conditions and lay down liquidation strategies considering the composition of the reserve assets.

SIO-11.3.12 The redemption plan must include the activation and operationalization timeline. Upon the CBB's decision to activate the redemption plan, the stablecoin issuer must operationalize the redemption plan without undue delay.

MODULE	SIO: Stablecoin Issuance & Offering
CHAPTER	SIO-12 Change in Substantial Shareholding, Control & Business Transfer

SIO-12.1 Change in Substantial Shareholding

SIO-12.1.1 **Any person or persons, acting in concert who intends to acquire, directly or indirectly, shares in a stablecoin issuer by virtue of which the person(s) would, if the acquisition is carried out, become a substantial shareholder of the stablecoin issuer , must obtain the approval of the CBB, prior to entering into an agreement with the stablecoin issuer.**

SIO-12.1.2 In Paragraph SIO-12.1.1 "substantial shareholder" means a person who alone or together with his associates:

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

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

SIO-12.1.3 **Any person applying for approval under Paragraph SIO-12.1.1 must submit to the CBB a written application along with supporting documents that sets out:**

(a) The name of the applicant;

(b) In the case where the applicant is a company:

(i) Its place of incorporation;

(ii) Its substantial shareholders;

(iii) Its directors and chief executive officer; and

(iv) Its principal business.

(c) In the case where the applicant is a natural person:

(i) Person's nationality;

(ii) Person's occupation; and

(iii) Details regarding directorship in company;

(d) List of all the companies in which the applicant has a substantial shareholding;

(e) The percentage of shareholding and voting power that the applicant has in the stablecoin issuer;

(f) The percentage of shareholding and voting power the applicant is seeking to have in the stablecoin issuer;

(g) The reasons for making the application;

(h) The mode and structure, as appropriate, under which the increase in shareholding would be carried out;

(i) Information relating to the financing of the proposed acquisition;

(j) Whether the applicant will seek representation on the board of directors of the stablecoin issuer; and

(k) Any other information that may facilitate the determination of the CBB as to whether the applicant is a fit and proper person for the purposes of Paragraph SIO-12.1.5 (a).

SIO-12.1 Change in Substantial Shareholding (continued)

SIO-12.1.4 The CBB may require the applicant to furnish it with such information or documents as the CBB considers necessary in relation to the application and the applicant shall furnish such additional information or documents as required by the CBB.

SIO-12.1.5 The CBB may approve an application made under Paragraph SIO-12.1.1 of this Module if the CBB is satisfied that:

(a) The applicant is a fit and proper person to be a substantial shareholder;
(b) Having regard to the applicant's likely influence, the stablecoin issuer will or will continue to conduct its business prudently and in compliance with the provisions of this Module; and
(c) It would not be contrary to the interests of the public to do so.

SIO-12.1.6 Where the CBB, based on its assessment, concludes that the proposed acquisition is not in the interest of the market, it shall reject the application and notify the applicant and provide reasons for its decision.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-12	Change in Substantial Shareholding, Control & Business Transfer

SIO-12.2 Business Transfer

SIO-12.2.1 **A stablecoin issuer must seek prior written approval from the CBB before transferring any of its business to a third party.**

SIO-12.2.2 **The CBB's approval to transfer business will only be given where:**

(a) **The transfer of business will not damage or otherwise prejudice the legitimate interests of the stablecoin issuer's clients;**

(b) **The transferee is duly licensed to undertake the business which it is to receive; and**

(c) **The CBB is satisfied that the transfer will not breach any applicable laws or regulations and would not create any supervisory concerns.**

SIO-12.2.3 In assessing the criteria outlined in Paragraph SIO-12.2.2, the CBB will, amongst other factors, take into account the financial strength of the transferee; its capacity to manage the business being transferred; its track record in complying with applicable regulatory requirements; and (where applicable) its track record in treating clients fairly. The CBB will also take into account the impact of the transfer on the transferor, and any consequences this may have for the transferor's remaining clients.

SIO-12.2.4 **A stablecoin issuer seeking to obtain the CBB's permission to transfer business must apply to the CBB in writing, in the form of a covering letter together with supporting attachments. Unless otherwise directed by the CBB, the application must provide:**

(a) **Full details of the business to be transferred;**

(b) **The rationale for the proposed transfer;**

(c) **If applicable, an assessment of the impact of the transfer on any clients directly affected by the transfer, and any mitigating factors or measures;**

(d) **If applicable, an assessment of the impact of the transfer on the transferor's remaining business and clients, and any mitigating factors or measures; and**

(e) **Evidence that the proposed transfer has been duly authorised by the transferor (such as a certified copy of a Board resolution approving the transfer).**

SIO-12.2.5 Stablecoin issuers intending to apply to transfer business are advised to contact the CBB at the earliest possible opportunity, prior to submitting a formal application, in order that the CBB may determine the nature and level of documentation to be provided and the need for an auditor or other expert opinion to be provided to support the application. The documentation specified in Paragraph SIO-12.2.4 may be varied by the CBB, depending on the nature of the proposed transfer, such as the materiality of the business concerned and its impact on customers.

SIO-12.2 Business Transfer (continued)

SIO-12.2.6 The CBB's approval may be given subject to any conditions deemed appropriate by the CBB. In all cases where additional requirements are imposed, the CBB shall state the reasons for doing so.

SIO-12.2.7 At its discretion, the CBB may require that a notice of proposed transfer of business be published in the Official Gazette, and/or in at least two local daily newspapers (one in Arabic, the other in English), in order to give affected clients, the right to comment on the proposed transfer. Where such a requirement has been imposed, the CBB's decision on the application will also be published in the Official Gazette and in at least two local daily newspapers. In all such cases, the costs of publication must be met by the transferor.

SIO-12.2.8 Publication under Paragraph SIO-12.2.7 will generally only be required where a proposed transfer involves a large number of clients or is otherwise deemed necessary in order to protect customer interests.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-12	Change in Substantial Shareholding, Control & Business Transfer

SIO-12.3 Change in Control

SIO-12.3.1 Any person seeking to acquire control of a stablecoin issuer must seek prior written approval of the CBB.

SIO-12.3.2 For the purposes of rule Paragraph SIO-12.3.1, "control" means the right to appoint the majority of the directors or to control the management or policy decisions exercisable by a person or persons acting individually or in concert, directly or indirectly, including by virtue of their shareholding or management rights or shareholders agreements or voting agreements, or in any other manner.

SIO-12.3.3 For the purposes of Paragraph SIO-12.3.1, a person(s) seeking to acquire control must request for the CBB's approval for taking control over a stablecoin issuer or taking any action that may lead to control by submitting Form 2 and shall also contain such particulars and information and be accompanied by such documents as the CBB may specify.

SIO-12.3.4 The CBB shall, within 60 days from the date of receipt of the request referred to in Paragraph SIO-12.3.3, notify the person intending to take control over a stablecoin issuer of its approval of control, any of the actions which would lead to control, or the refusal thereof as the CBB may determine at its own discretion.

SIO-12.3.5 The CBB may impose any restrictions that it considers necessary to be observed in case of its approval of control, or any of the actions that would lead to control.

SIO-12.3.6 The person intending to take control over a stablecoin issuer, may within 30 days of the notification referred to in Paragraph SIO-12.3.4, lodge a grievance against the CBB's decision to refuse the control or any conditions imposed in respect of such control. The CBB shall decide on the grievance and notify the person intending to take control over the stablecoin issuer of its decision within 30 days from the date of submitting the grievance.

SIO-12.3.7 The CBB may refuse to give approval for change of control, if the CBB, based on its own assessment, concludes that the change in control would adversely affect financial stability, market integrity and interests of the clients, or if the CBB decides that the person(s), do not meet the fit and proper requirement set by the CBB.

SIO-12.3.8 Any person who acquires control or shares in breach of the provisions of this Module shall carry out any instructions issued to him by the CBB to transfer such control or shares, or refrain from exercising control or voting rights according to the procedures prescribed in such instructions.

SIO-12.3.9 A stablecoin issuer must not perform any of the following without prior written approval of the CBB:

(a) Merge, amalgamate or enter into a partnership with any person in Bahrain or elsewhere, except in the ordinary course of business;

(b) Transfer all or a major part of its assets or liabilities in Bahrain or elsewhere, without prejudice to the provisions of Chapter 6 (Articles 66, 67 & 68) of the CBB Law;

(c) Make any modification to its issued or paid-up share capital;

(d) Modify its Memorandum and Articles of Association;

(e) Engage in major acquisition or investment operations as determined by the CBB.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-13	Information Gathering by the CBB

SIO-13.1 Power to Request Information

SIO-13.1.1 **Stablecoin issuers must provide all information that the CBB requests in order to discharge its regulatory obligations.**

SIO-13.1.2 **Stablecoin issuers 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 stablecoin issuers 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 enforcement measures.**

SIO-13.1.3 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 stablecoin issuer.

SIO-13.2 Access to Premises

SIO-13.2.1 Representatives of the CBB, or persons appointed by the CBB for investigation purposes may access, with or without notice, any of the stablecoin issuer's business premises in relation to the discharge of the CBB's functions pursuant to the CBB Law.

SIO-13.2.2 A stablecoin issuer must take reasonable steps to ensure that its agents and providers under outsourcing arrangements permit such access to their business premises, to the CBB.

SIO-13.2.3 A stablecoin issuer 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 stablecoin issuer.

SIO-13.2.4 The cooperation that stablecoin issuers are expected to procure from such providers is similar to that expected of stablecoin issuers themselves.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-13	Information Gathering by the CBB

SIO-13.3 Accuracy of Information

SIO-13.3.1 **A stablecoin issuer must ensure that all information it provides to the CBB is:**

(a) Factually accurate or, in the case of estimates and judgements, fairly and properly based on appropriate analysis and enquiries have been made by the stablecoin issuer; and

(b) Complete, in that it should include everything which the CBB would reasonably and ordinarily expect to have or require.

SIO-13.3.2 **If a stablecoin issuer 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 of why such information was or may have been provided in false, misleading, incomplete or inaccurate manner; and

(c) The correct information.

SIO-13.3.3 **If the information in Paragraph SIO-13.3.2 cannot be submitted with the notification (because it is not immediately available), it must instead be submitted as soon as possible afterwards.**

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-13	Information Gathering by the CBB

SIO-13.4 Methods of Information Gathering

SIO-13.4.1 The CBB uses various methods of information gathering on its own initiative which require the cooperation of stablecoin issuers:

(a) Representatives of the CBB may make onsite visits at the premises of the stablecoin issuer. 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 stablecoin issuers), or when the CBB has a particular reason for visiting a stablecoin issuer;

(b) Appointees of the CBB may also make onsite visits at the premises of the stablecoin issuer. Appointees of the CBB may include persons who are not CBB staff, but who have been appointed to undertake particular tasks or activities for the CBB, such as in the case of Appointed Experts (refer to Section SIO-13.5).

(c) The CBB may request the stablecoin issuer 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 stablecoin issuers to submit various documents or notifications, as per Chapter SIO-13, in the ordinary course of their business such as reports or upon the occurrence of a particular event in relation to the stablecoin issuer such as a change in control.

SIO-13.4.2 When seeking meetings with a stablecoin issuer or access to the stablecoin issuer's premises, the CBB or the CBB appointee will access a stablecoin issuer's documents and personnel. Such requests will normally be made during reasonable business hours and with proper notice. However, there may be instances where the CBB may access the stablecoin issuer's premises without prior notice.

SIO-13.4.3 The CBB expects that a stablecoin issuer should:

(a) Make itself readily available for meetings with representatives or appointees of the CBB;

(b) Give representatives or appointees of the CBB access to any records, files, tapes or computer systems, which are within the stablecoin issuer'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 stablecoin issuer's possession or control requested or required;

(d) Print information in the stablecoin issuer's possession or control which is held on computer or otherwise convert it into a readily legible document or any other record which the CBB may reasonably request;

(e) Arrange for representatives or appointees of the CBB to copy documents or other material on the premises of the stablecoin issuer at the stablecoin issuer's expense and to remove copies and hold them elsewhere, or provide any copies, as requested by the CBB or its appointees; and

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

SIO-13.4 Methods of Information Gathering

SIO-13.4.4 The CBB considers that a stablecoin issuer should ensure that the following persons act in the manner set out in Paragraph SIO-13.4.3:

(a) Its employees; and

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

MODULE	SIO: Stablecoin Issuance & Offering
CHAPTER	SIO-13 Information Gathering by the CBB

SIO-13.5 The Role of the Appointed Expert

SIO-13.5.1 The content of this Chapter is applicable to all stablecoin issuers and appointed experts.

SIO-13.5.2 The purpose of the contents of this Chapter is to highlight the roles and responsibilities of appointed experts when appointed pursuant to Articles 114 or 121 of the CBB Law.

SIO-13.5.3 The CBB uses its own inspectors to undertake on-site examinations of stablecoin issuers as an integral part of its regular supervisory role. In addition, the CBB may commission reports on matters relating to the business of stablecoin issuers in order to assist it in assessing their compliance with CBB requirements.

SIO-13.5.4 Appointed experts must not be the same firm appointed as external auditor of the stablecoin issuer.

SIO-13.5.5 The CBB will decide on the range, scope and frequency of work to be carried out by appointed experts.

SIO-13.5.6 The appointment of an appointed expert will be made in writing directly with the appointed experts concerned. A separate letter is sent to the stablecoin issuer, 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 stablecoin issuer and the appointed experts, to discuss any aspect of the inspection or investigation or the report produced by the appointed expert.

SIO-13.5.7 Following the completion of the investigation, the CBB will normally provide feedback on the findings of the investigation to the stablecoin issuer.

SIO-13.5.8 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 stablecoin issuer's group structure). The report produced by the appointed experts is the property of the CBB.

SIO-13.5.9 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 stablecoin issuer (i.e. create a conflict of interest).

SIO-13.5.10 The CBB may appoint one or more of its officials to work with the appointed experts' team for a particular stablecoin issuer.

SIO-13.5 The Role of the Appointed Expert (continued)

The Required Report

SIO-13.5.11 The scope of the required report will be determined and detailed by the CBB in the appointment letter. Appointed experts would normally be required to report on one or more of the following aspects of a stablecoin issuer'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.

SIO-13.5.12 Appointed experts will be required to form an opinion on whether, during the period examined, the stablecoin issuer is in compliance with the relevant provisions of the CBB Law and the CBB's other requirements, as well as other requirements of Bahrain Law and, where relevant, industry best practice locally and/or internationally.

Other Notifications to the CBB

SIO-13.5.13 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 that 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 stablecoin issuer, or that the interests of clients are at risk because of adverse changes in the financial position or in the management or other resources of the stablecoin issuer. Notwithstanding the above, it is primarily the stablecoin issuer's responsibility to report such matters to the CBB.

Permitted Disclosure by the CBB

SIO-13.5.14 Appointed experts must keep all information relating to the stablecoin issuer confidential and not divulge it to a third party except with the CBB's written permission or unless required by applicable laws in the Kingdom of Bahrain.

SIO-14.1 General Procedures

The CBB's Approach to Enforcement

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

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

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

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

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

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

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

SIO-14.1 General Procedures (continued)

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

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

Prohibition on Insurance

SIO-14.1.9 To help the CBB achieve the purpose of this Module, stablecoin issuers 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 fines provided for in this Module.

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

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

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

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

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

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-14	Enforcement

SIO-14.2 Formal Warning

CBB Policy

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

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

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

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

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

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

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

Procedure for Issuing Formal Warnings

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

SIO-14.2.5 Depending on the issue in question, recipients of a formal warning may be required to respond to the contents of the warning. In any case, recipients have the right to object to or challenge a formal warning as specified under Articles 125(c) and 126 of the CBB Law.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-14	Enforcement

SIO-14.3 Directions

CBB Policy

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

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

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

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

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

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

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

Procedure for Issuing Directions

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

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

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-14	Enforcement

SIO-14.3 Directions (continued)

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

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-14	Enforcement

SIO-14.4 Formal Request for Information

Procedure for request of Information

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

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

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

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

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

SIO-14.5 Adverse "Fit and Proper" Findings

Requirements for Individuals

SIO-14.5.1 Article 65 of the CBB Law, allows the CBB to determine the level of qualifications, experience, and training of board members, officers or employees.

SIO-14.5.2 In addition, Section SIO-2.7 specifies that all persons wishing to hold or holding the position of Director, Chief Executive/General Manager or Manager in a stablecoin issuer must be assessed by the CBB as "fit and proper" to hold such a position. The section specifies various factors that the CBB takes into account when reaching such a decision.

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

CBB Policy

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

(a) The extent to which the factors set out in Section SIO-2.7 have not been met;
(b) The extent to which the person has deliberately or recklessly breached requirements of the CBB Law and/or this Module;
(c) The person's past compliance record and conduct following any such contravention;
(d) The length of time since factors indicating a lack of fitness or propriety occurred; and
(e) The risk the person poses to the stablecoin issuer and its clients.

SIO-14.5.5 In assessing evidence, the CBB applies a lower threshold than is applied in a criminal court of law, reflecting generally, the administrative nature of the sanction. The CBB may also take into account the cumulative effect of factors which, when considered individually, may not in themselves be sufficient to justify an adverse "fit and proper" finding.

SIO-14.5.6 The CBB may also take into account the particular function being undertaken in the licensee by the individual concerned, and the size and nature of the stablecoin issuer itself, particularly when assessing the suitability of a person's experience or qualifications. Thus, the fact that a person was deemed "fit and proper" for a particular position in a particular firm does not necessarily mean he would be suitable in a different position or in a different firm.

SIO-14.5.7 The CBB may carry out re-assessment tests in case of individuals deemed to be responsible for serious or repeated violations (refer to Appendix E).

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

Procedure for Issuing an Adverse Finding

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

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

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

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-14	Enforcement

SIO-14.6 Financial Penalties

CBB Policy

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

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

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

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

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

(a) Failures to address persistent delays and/or significant inaccuracies in regulatory reporting to the CBB;
(b) Repeated failures to respond to formal requests for information from the CBB, within the deadlines set;
(c) The submission of information to the CBB known to be false or misleading; and
(d) Major failures in maintaining adequate systems and controls in accordance with the CBB's requirements, subjecting depositors and other customers to significant risk of financial loss.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-14	Enforcement

SIO-14.6 Financial Penalties (continued)

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

(a) The seriousness of the contravention, in relation to the requirement(s) concerned;
(b) The duration and/or frequency of the contravention, and the extent to which it reflects more widespread weaknesses in controls and/or management; the extent to which the contravention was deliberate or reckless;
(c) The licensee's past compliance record and conduct following the contravention; and
(d) The scope of any other action taken by the CBB or other regulators against the stablecoin issuer, in response to the compliance failures in question.

Additional criteria are set out in Appendix E.

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

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

(a) The violations committed by the stablecoin issuer with respect to CBB Law; or the prudential Rulebook; or any Directions, warnings or formal requests for information; or violations of the terms and conditions of the license issued to the stablecoin issuer;
(b) Evidence or proof to support the above;
(c) The level of financial penalty to be imposed; and
(d) The grace period to be allowed to the stablecoin issuer for challenging the intended penalty (which will not be less than 30 days).

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

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

Financial Penalties for Date Sensitive Requirements

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

SIO-14.6 Financial Penalties (continued)

SIO-14.6.12 This Section applies to date sensitive requirements for:
a. Reporting requirements included in this Module;
b. Public disclosure requirements included in this Module;
c. The report of the external auditor or a consultancy firm approved by the CBB required as per Paragraph AML-3.3.1B(d) of Module AML;
d. Annual licensing fees required as per Section SIO-2.6, and
e. Conduct of Shareholders' Meetings requirements included in Section HC 10.7.

SIO-14.6.13 Financial penalties related to late filing or other date sensitive requirements are calculated on per diem basis. The financial penalty for late filing is BD 100 per day.

SIO-14.6.14 The various deadlines for submission of reports and annual fees referred to in this Module are defined:
(a) In terms of a specified number of days or months following a given date, such as the last date of a calendar quarter;
(b) A specified number of days or months after the occurrence of a specific event; or
(c) A specific date.

SIO-14.6.15 In imposing financial penalties for date sensitive requirements, the following criteria apply:
(a) Where the due date falls on a weekend or a holiday as designated by the CBB, the first business day following the weekend or holiday will be considered as being the due date;
(b) Where a due date is not complied with by the end of the day on which it is due, holidays and weekend days are included in the number of days the item is considered late;
(c) For returns and other filings, the date received is the date recorded by the CBB's systems in case of returns filed electronically;
(d) In the case of returns filed in hard copy, the CBB stamp is the date received;
(e) All returns are to be sent to the respective Supervision Directorate and the annual fees to the Accounts Directorate, on or before the due date, to be considered filed on time;
(f) A day ends at midnight in the case of returns that must be filed electronically, or at the close of CBB business day, in the case returns are filed in hard copy; and
(g) An incomplete return, where completeness is determined in relation to the requirements of the relevant instructions, is considered 'not filed' until the CBB receives all necessary elements of the return.

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

SIO-14.6 Financial Penalties (continued)

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

Procedures for Financial Penalties

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

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

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

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

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

SIO-14.6 Financial Penalties (continued)

Remedying a Compliance Failure

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

SIO-14.7 Investigation

CBB Policy

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

SIO-14.7.2 Failure by stablecoin issuers to cooperate fully with the CBB's inspectors or appointed experts, or to respond to their examination reports within the time limits specified, will be treated as demonstrating a material lack of cooperation with the CBB which will result in other enforcement measures being considered, as described elsewhere in this Module. This Rule is supported by Article 124(a) of the CBB Law.

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

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

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

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

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

SIO-14.7.8 Further details on the required report and other aspects related to the role of the appointed expert are contained in Section SIO-13.5.

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-14	Enforcement

SIO-14.8 Administration

Legal Source

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

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

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

CBB Policy

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

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

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

SIO-14.8 Administration (continued)

(d) The extent to which the licensee has contravened the conditions of the CBB Law, including the extent to which the contraventions reflect more widespread or systemic weaknesses in controls and/or management.

Procedure for Implementing an Administration

SIO-14.8.7 All proposals for assuming the administration of a stablecoin issuer are subject to a thorough review by the CBB of all relevant facts, assessed against the criteria outlined in Section SIO 14.8.1 to SIO-14.8.3.

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

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

SIO-14.9 Cancellation or Amendment of License

Legal Source

SIO-14.9.1 Article 48 of the CBB Law empowers the CBB to cancel or amend a license under certain circumstances. These include cases where a stablecoin issuer has:

(a) Failed to satisfy its license conditions;
(b) Violated the terms of the CBB Law, CBB Regulations or this Module; or
(c) Failed to start business within six months from the date of the license;
(d) Ceased to carry out the licensed activities permitted; or
(e) Not acted in the legitimate interest of its customers or creditors.

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

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

SIO-14.9.4 The criteria used by the CBB in assessing whether to seek cancellation or amendment of a license include:

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

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

SIO-14.9 Cancellation or Amendment of License (continued)

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

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

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

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

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

MODULE	SIO:	Stablecoin Issuance & Offering
CHAPTER	SIO-14	Enforcement

SIO-14.10 Criminal Sanctions

Overview

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

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

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

CBB Policy

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

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

Articles of CBB Law

Article 161

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

SIO-14.10 Criminal Sanctions (continued)

Article 163

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

(a) Conceals any records, information or documents requested by the CBB (or any person appointed by the CBB to conduct an investigation or inspection);
(b) Provides statements or information in bad faith which do not reflect the actual financial position of the stablecoin issuer;
(c) Conceals from an external auditor any records, information or documents necessary for auditing the accounts of the stablecoin issuer; and
(d) Provides in bad faith any misleading or inaccurate statements to an external auditor which do not reflect the actual financial position of the stablecoin issuer.

Article 169

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

Article 170

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

Article 171

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