STABLECOINS ORDINANCE

Guideline on
Supervision of Licensed Stablecoin Issuers

August 2025

Table of Contents

1. Introduction

1.1. This Guideline on Supervision of Licensed Stablecoin Issuers is issued pursuant to section 171(4) of the Stablecoins Ordinance ("SO") to set out guidance on the Hong Kong Monetary Authority ("HKMA")'s expectations with regard to the minimum criteria in Schedule 2 to the SO which a licensee is required to fulfil on an ongoing basis pursuant to section 24 of the SO.

1.2. This Guideline should be read in conjunction with the SO as well as other guidance issued by the HKMA from time to time. Unless otherwise defined in the Glossary of this Guideline, terms used in this Guideline shall have the same meaning as those defined in the SO. Unless otherwise specified, terms in this Guideline in the singular include the plural and terms in this Guideline in the plural include the singular. In this Guideline, use of the word "must" indicates a statutory requirement whereas "should" indicates the HKMA's regulatory expectations.

1.3. The relevance and usefulness of this Guideline will be kept under review and it may be necessary to issue amendments from time to time.

2. Reserve assets management

2.1. Overview

2.1.1. A licensee should put in place a set of policies and procedures for managing its reserve assets. The policies and procedures should set out, among other things, (i) a governance arrangement with clear reporting lines and sufficient segregation of duties, (ii) detailed measures adopted for fulfilling requirements in relation to reserve assets management, and (iii) detailed procedures for carrying out operations with stringent authorisation control.

2.2. Full backing

2.2.1. Section 5(2) of Schedule 2 to the SO stipulates that a licensee must implement measures to ensure that in relation to each type of specified stablecoins it issues, the market value of the specified reserve assets pool backing the type of specified stablecoins is at all times at least equal to the par value of the outstanding specified stablecoins of the type in circulation. In practice, the licensee should take into account the risk profile of the reserve assets, and ensure that there is appropriate over-collateralisation to provide adequate buffer above the full backing level (see paragraphs 2.4.1 and 6.4.5). The licensee should also ensure that the custodial arrangement in respect of the reserve assets will not compromise its full backing (e.g. ensuring that account-level fees would not be deducted from accounts in which reserve assets are held). Furthermore, the licensee should ensure that measures are implemented for monitoring and conducting regular reconciliation between the market value of the reserve assets and the par value of the outstanding specified stablecoins in circulation to verify that the full backing requirement is fulfilled.

2.2.2. A licensee should ensure that a consistent and prudent approach is adopted in calculating the market value of reserve assets. The calculation method and the sources of the market prices should be reasonable, reliable, and able to reflect prevailing market prices, and the valuation should be conducted at the bid price which is the more prudent price for the sale of a financial asset where applicable. The licensee should also ensure that a consistent and transparent approach is taken in calculating the par value of the outstanding specified stablecoins in circulation, and that there is no mismatch between the approaches for calculating market value of reserve assets and par value of the outstanding specified stablecoins in circulation.

2.2.3. For the avoidance of doubt, a licensee should ensure that specified stablecoins that are temporarily restricted from being accessed, transferred and redeemed by specified stablecoin holders (e.g. specified stablecoins that are frozen due to

enforcement actions or court orders but could potentially be unfrozen after court order or investigation) are fully backed, so that the licensee would be able to meet redemption requirements in accordance with paragraph 3 once the restrictions are no longer in force.

2.3. Scope and composition of reserve assets

2.3.1. Section 5(5) of Schedule 2 to the SO stipulates that reserve assets must be of high quality and high liquidity with minimal investment risks. Reserve assets should be held in the form of:

(i) Cash;

(ii) Bank deposits with a term of no longer than three (3) months;

(iii) Marketable debt securities that:

a. Are issued or guaranteed by a government, central bank, public sector entity, qualified international organisation or multilateral development bank;

b. Have residual maturity of no longer than one (1) year;

c. (I) Qualify, in the calculation of credit risk under the standardized (credit risk) approach, for a 0% risk weight pursuant to sections 55 to 58 of the Banking (Capital) Rules (Cap. 155L); or (I) are denominated in the domestic currency of the issuer that is a government or central bank;

d. Are of high liquidity; and

e. Are not an obligation of a financial institution or an associated entity of a financial institution, that is not a public sector entity bank;

(iv) Cash receivable from overnight reverse repurchase agreements with minimal counterparty risk, collateralised by assets set out in (iii);

(v) Investment funds that invest in assets set out in (i), (ii), (iii) and/or (iv), where such investment funds should be set up dedicated for the sole purpose of managing the reserve assets of a licensee; and/or

(vi) Other types of assets which are acceptable to the HKMA.

Collectively, the "eligible assets".

2.3.2. For the avoidance of doubt, the reserve assets may consist of the tokenised representations of the eligible assets. To this end, a licensee should demonstrate to the satisfaction of the HKMA how the concerned tokenised representations of the eligible assets fulfil the requirement of high quality, high liquidity and minimal investment risks.

2.4. Referenced currency

2.4.1. Section 5(3) of Schedule 2 to the SO stipulates that except with the prior written approval of the Monetary Authority, the specified reserve assets pool for each type of specified stablecoins issued by a licensee must be held in the same reference asset as that referenced by the type of specified stablecoins. Reserve assets should be denominated in the respective referenced currency of the specified stablecoins issued by the licensee, or if there is more than one referenced currency, denominated in the referenced currencies in the same ratio as that to which the specified stablecoins are referenced, with flexibility allowed on a case-by-case basis, subject to prior written approval of the Monetary Authority. When determining whether approval should be given to allow flexibility in respect of currency mismatch, the HKMA would consider whether there is a legitimate reason for having a currency mismatch, whether the licensee is able to demonstrate the needs and rationale for doing so, and whether the proposed arrangements (including for example the composition and proportion of reserve assets, as well as corresponding risk mitigating measures such as over over-collateralisation) are reasonable and can effectively manage the relevant risks so as to avoid transferring such risks to the specified stablecoin holders or negatively impacting its operations.

2.5. Segregation and safekeeping

2.5.1. Sections 5(1) and 5(4) of Schedule 2 to the SO set out the minimum criteria with regard to the segregation and safekeeping of reserve assets. A licensee must ensure that the reserve assets for each type of specified stablecoins it issues are (i) segregated from any other pools of reserve assets it maintains, (ii) adequately protected against claims by its other creditors in all circumstances, and (iii) kept separate from other assets of the licensee, including any other funds paid to, maintained or received by the licensee.

2.5.2. Effective trust arrangements should be put in place to ensure that the reserve assets are segregated from the assets of a licensee, held for and on behalf of specified stablecoin holders, and are available to satisfy specified stablecoin holders' valid redemption requests at par value (see paragraph 3.3). In this regard, the appointment of an independent trustee or a declaration of trust over the reserve assets would be considered as an acceptable trust arrangement. Prior

to any implementation of a trust arrangement, the licensee should obtain an independent legal opinion demonstrating the effectiveness of the trust arrangement, and submit the same to the HKMA. If there are any material changes to a trust arrangement, the licensee should submit an updated independent legal opinion to the HKMA accordingly.

2.5.3. Any income or loss generated from the management of reserve assets should be attributed to a licensee (see paragraph 2.6). The trust arrangement under which the reserve assets are held should include an arrangement to facilitate the regular transfer of excess assets (i.e. the portion of assets that exceed the internal target set out by the licensee) from the account of reserve assets to the licensee's own account. The arrangement should consist of a triggering mechanism, as well as detailed procedures to ensure that the transfer involves only the excess assets. In addition, the prescribed trust arrangement should also cater for a potential triggering of the licensee's business exit plan (see paragraph 6.8.17).

2.5.4. Section 5(8) of Schedule 2 to the SO sets out the minimum criteria in relation to the engagement of third party entities with regard to reserve assets management. To this end, qualified custodians should be appointed for the safekeeping of reserve assets. A custodian should be a licensed bank, or other asset custodian under an arrangement which is acceptable to the HKMA. In case investment managers are being engaged for the purpose of management of reserve assets, a licensee should also ensure that the investment managers are qualified for such role. When conducting risk assessments and due diligence on a prospective custodian and/or investment manager in accordance with the requirements set out in paragraph 6.6 on third party risk management, factors including but not limited to its size, capabilities, expertise, track record, reputation, as well as presence in Hong Kong should be taken into account. Notwithstanding the appointment of custodians and/or investment managers (if any), the licensee should be primarily responsible and accountable for the proper management and safekeeping of reserve assets.

2.6. Non-interest bearing

2.6.1. Section 15 of Schedule 2 to the SO stipulates that a licensee must not pay, or permit to be paid, any interest in relation to the specified stablecoins it issues. A licensee should not pay interest or interest-like incentive in any form to specified stablecoin holders, save that a licensee may offer marketing incentives that do not amount to payment of interest. To this end, interest means any profit, income or other return represented to arise or to be likely to arise from the holding of the specified stablecoins on the basis of (i) the length of the period during which the holder holds the specified stablecoins, (ii) the par value of the specified stablecoins, or (iii) the market value of the specified stablecoins. In addition, the licensee should ensure that any income or loss arising from the

management of reserve assets, including but not limited to interest payments or capital gains or losses, is attributed to the licensee.

2.7. Disclosure and reporting

2.7.1. Section 5(7) of Schedule 2 to the SO stipulates that a licensee must disclose to the public, among other things, its reserve assets management policy, the composition and market value of its reserve assets as well as the results of regular independent attestation and audit of its reserve assets. Paragraph (b) of section 5(6) of Schedule 2 to the SO sets out the minimum criteria with regard to the systems of control on independent attestation and audit.

2.7.2. To this end, on a daily basis, a licensee should prepare statements on the par value of the outstanding specified stablecoins in circulation, as well as the market value and composition of its reserve assets, and such statements should be ready for submission to the HKMA as and when requested. Unless otherwise agreed by the HKMA, the licensee should report to the HKMA on a weekly basis and update at a reasonably prominent location on its website the aforementioned information.

2.7.3. A licensee should engage a qualified and independent external auditor that is acceptable to the HKMA to perform attestation on a regular basis at a frequency that is acceptable to the HKMA, on: (i) the market value and composition of its reserve assets, (ii) the par value of the outstanding specified stablecoins in circulation, and (iii) whether its reserve assets are adequate to fully back the par value of the outstanding specified stablecoins in circulation as of the last business day of the period covered by the attestation report, and as of at least one randomly selected business day during such period. The licensee should submit the attestation report to the HKMA within one month following the last business day of the period covered by the attestation report, and disclose each attestation report to the public at a reasonably prominent location on its website.

2.7.4. A licensee's annual financial audit should cover its reserve assets (see paragraph 8.2.5). Separately, the licensee should review its reserve assets management policies and procedures regularly and at least on a quarterly basis. Any shortcomings identified during such review should be promptly addressed and reflected in the updated policies and procedures. The policies and procedures, as well as any material changes, should be approved by the board of directors ("Board"). The licensee should also conduct regular audits to assess whether its reserve assets are managed in compliance with the policies and procedures, as well as applicable regulatory requirements. The licensee should report the audit outcomes, including any material findings, to the HKMA in a timely manner and promptly provide the audit report and relevant supporting documents to the HKMA upon request.

2.7.5. If there is a breach of statutory or regulatory requirements in relation to reserve assets management, material non-compliance with reserve assets management policies (including those arising from third party arrangements), and unresolved discrepancies identified in any reconciliation exercise, such incidents should be reported to the HKMA immediately.

3. Issuance, redemption and distribution

3.1. Overview

3.1.1. A licensee should put in place a set of policies and procedures for issuance, redemption and distribution of the specified stablecoins it issues. The policies and procedures should set out, among other things, (i) a governance arrangement with clear reporting lines and sufficient segregation of duties, (ii) detailed measures adopted for fulfilling requirements in relation to issuance, redemption and distribution, and (iii) as part of its overall internal control system, detailed procedures for carrying out operations with stringent authorisation control.

3.2. Issuance requirements

3.2.1. Section 11 of Schedule 2 to the SO stipulates that the issue of a specified stablecoin by a licensee must be prudent and sound, having regard to the purpose, business model and operational arrangement of the issue. To this end, the licensee should establish and maintain an effective issuance mechanism for specified stablecoins it issues. In practice, the licensee should issue specified stablecoins only to its customers (see paragraph 3.5), and the issuance should be carried out as soon as practicable after receiving the funds and a valid issuance request. The funds received from customers as part of the issuance process should be denominated in the respective referenced currency of the specified stablecoins issued by the licensee, or if there is more than one referenced currency, denominated in the referenced currencies in the same ratio as that to which the specified stablecoins are referenced. Any minting of specified stablecoins during the process should be matched by a corresponding increase in the relevant reserve assets pool.

3.3. Redemption requirements

3.3.1. Section 6 of Schedule 2 to the SO sets out the minimum criteria with regard to the redemption of specified stablecoins. A licensee must provide specified stablecoin holders with a right to redeem the specified stablecoins at par value. The licensee must also, in respect of each type of specified stablecoins issued by it, provide each specified stablecoin holder with (i) a right to direct the disposal of the specified reserve assets pool for the purpose of redeeming all outstanding specified stablecoins of that type on a pro rata basis, as well as (ii) a right to claim against the licensee for any shortfall if the proceeds from the disposal of the specified reserve assets pool is insufficient to redeem all the

outstanding specified stablecoins of that type in full. The rights mentioned in items (i) and (ii) must be exercisable in the event of the licensee's insolvency.

3.3.2. A licensee should obtain an independent legal opinion to demonstrate that it has provided specified stablecoin holders with the rights set out in paragraph 3.3.1. The licensee should submit the independent legal opinion to the HKMA. If there are any material changes to such rights of specified stablecoin holders, the licensee should submit an updated independent legal opinion to the HKMA accordingly.

3.3.3. A licensee should establish and maintain an effective redemption mechanism for the specified stablecoins it issues. Valid redemption requests made by a specified stablecoin holder must be honoured by the licensee, without charging an unreasonable fee in connection with redemption or attaching any unduly burdensome condition, as soon as practicable, except with the prior written consent of the Monetary Authority. Unless otherwise approved, valid redemption requests should be processed within one (1) business day after the day on which it is received by the licensee.

3.3.4. In evaluating the reasonableness of the fees charged, factors including but not limited to the proportionality of fees to the operational costs of processing the redemption requests by a licensee, as well as prevailing industry practices will be taken into account. In assessing whether a condition is unduly burdensome, factors taken into account may include but are not limited to whether fulfilment of the condition is reasonably practicable, whether the condition is imposed due to certain legal or regulatory obligations of the licensee, and whether the condition would cause undue hardship to specified stablecoin holders.

3.3.5. To honour a valid redemption request, a licensee should transfer funds in an amount equal to the par value of the specified stablecoins received from the specified stablecoin holder, after deducting any fees as mentioned in paragraph 3.3.3, to the specified stablecoin holder. The funds should be denominated in the respective referenced currency of the specified stablecoins issued by the licensee, or if there is more than one referenced currency, denominated in the referenced currencies in the same ratio as that to which the specified stablecoins are referenced. The licensee should ensure that a draw-down of its reserve assets for honouring a redemption request is matched by a corresponding decrease in the par value of the outstanding specified stablecoins in circulation.

3.4. Distribution requirements

3.4.1. Section 11 of Schedule 2 to the SO stipulates that the issue of a specified stablecoin by a licensee must be prudent and sound, having regard to the purpose, business model and operational arrangement of the issue. While the business model and operational arrangements may differ among licensees, if a licensee

enters into arrangements with third party entities for the distribution of the specified stablecoins it issues, it should ensure that such arrangements will not adversely affect the prudence and soundness of its issuances.

3.4.2. In practice, a licensee should consider the laws and regulations of the relevant jurisdictions, as well as the licensing status of the third party entities involved to address the legal and compliance risks. In particular, if the third party entities offer specified stablecoins in Hong Kong, the licensee should ensure that the third party entities are permitted offerors. In addition, when conducting risk assessments and due diligence on the third party entities in accordance with the requirements set out in paragraph 6.6 on third party risk management, the licensee should consider factors including but not limited to the size, capabilities, expertise, track record and reputation of the third party entities, as well as the adequacy of the governance, conduct, risk management, and internal control measures implemented by the third party entities. Furthermore, the licensee should also ensure that the arrangements with third party entities comply with the relevant laws and regulations in the concerned jurisdictions. Specifically, the arrangements should not involve distribution of the specified stablecoins issued by the licensee in jurisdictions where such activity is unlawful.

3.4.3. For third party entities that provide liquidity in the secondary market for specified stablecoins issued by a licensee, the licensee should consider the need to engage such parties, and if so, the extent and scope of the arrangements, taking into account its business model and operational arrangement. The licensee should ensure that any of such arrangements have the goal of maintaining relatively stable value for the specified stablecoins in the secondary markets, and that any potential and/or actual conflicts of interest have been identified as well as properly addressed and mitigated.

3.5. Customer on-boarding and management

3.5.1. A licensee should establish adequate and effective policies and procedures for customer on-boarding in respect of issuance and redemption of specified stablecoins. If applicable, the licensee should carry out customer due diligence measures on specified stablecoin holders and/or potential specified stablecoin holders before issuance and redemption. For details, please refer to the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Stablecoin Issuers).

3.5.2. A licensee should comply with the relevant laws and regulations in the jurisdictions where it offers specified stablecoins, and a comprehensive set of policies and procedures should be put in place to manage this aspect by, including but not limited to, (i) ensuring that it does not issue or offer specified stablecoins in jurisdictions where such activity is unlawful (e.g. by verification of identity documents, geolocation lookup via Internet Protocol ("IP") addresses

or global positioning system, blocking access, etc.), (ii) ensuring that its operations and marketing activities are compliant with the applicable laws and regulations of the respective jurisdictions, and (iii) actively monitoring any policy changes and updates with respect to specified stablecoins in order to adjust its relevant operations.

3.5.3. A licensee should implement controls to mitigate the risk of location spoofing (e.g. via use of virtual private networks ("VPN")) during remote customer on-boarding as well as during its course of business. For example, the licensee may detect VPN usage by examining the network protocols, checking device configurations (e.g. timestamp, presence of VPN profiles), and/or verifying IP addresses against the server addresses of commercial VPN providers.

3.6. Disclosure and reporting

3.6.1. As set out in section 6(5) of Schedule 2 to the SO, a licensee must disclose to the public its redemption mechanism and procedures, redemption rights, timeframe, as well as the applicable conditions and fees involved, if any. Such information should be clearly set out in the white paper (see paragraph 8.2.3) as well the terms and conditions applicable to specified stablecoin holders. For the avoidance of doubt, the terms and conditions should apply to all specified stablecoin holders, regardless of whether a customer relationship has been established with the licensee. In addition, the terms and conditions should also address (i) the arrangement for issuance and redemption during exceptional circumstances, such as hard forks, and (ii) the transfer mechanism of the specified stablecoins (e.g. the point at which the specified stablecoins are considered being transferred as a specified stablecoin holder executes a transfer), having regard to the operations of the underlying distributed ledgers. The terms and conditions should be published at a reasonably prominent location on the licensee's website.

3.6.2. A licensee should review its issuance, redemption and distribution policies and procedures regularly and at least on an annual basis. Any shortcomings identified during such review should be promptly addressed and reflected in the updated policies and procedures. The policies and procedures, as well as any material changes, should be approved by the Board. The licensee should also conduct regular audits to assess whether its operations are in compliance with the policies and procedures, as well as the applicable regulatory requirements. The licensee should report the audit outcomes, including any material findings, to the HKMA in a timely manner and promptly provide the audit report and relevant supporting documents to the HKMA upon request.

3.6.3. If there is a breach of any statutory or regulatory requirements in relation to issuance, redemption and distribution, and material non-compliance with issuance, redemption and distribution policies (including those arising from

third party arrangements), such incidents should be reported to the HKMA immediately.

4. Business activities

4.1. Restrictions on business activities

4.1.1. Section 12 of Schedule 2 to the SO sets out the minimum criteria with regard to the conduct of business activities of a licensee. A licensee must obtain the Monetary Authority's consent before it carries on any business activity other than a licensed stablecoin activity ("Other Business Activities"). The licensee should establish clear governance arrangements for such Other Business Activities, conduct risk assessments to identify all relevant risks, as well as implement controls to properly manage and mitigate the identified risks. The licensee should demonstrate, and have adequate and appropriate systems of control to ensure, that the Other Business Activities will not pose significant risks to its licensed stablecoin activities and that potential or actual conflicts of interest from any Other Business Activities are properly managed and mitigated. The licensee must also ensure that sufficient resources are dedicated to its licensed stablecoin activities.

4.1.2. A licensee should also assess whether the Other Business Activities would constitute other regulated activities, and whether it is able to fulfil the requirements of all applicable regulatory regimes.

4.1.3. The requirements in paragraphs 4.1.1 and 4.1.2 do not apply to a licensee that is an authorized institution. A licensee that is an authorized institution should comply with requirements under the Banking Ordinance (Cap. 155) and relevant guidance.

4.2. Issuance of more than one type of specified stablecoins

4.2.1. Section 11 of Schedule 2 to the SO stipulates that the issue of specified stablecoins must be prudent and sound, having regard to the purpose, business model and operational arrangement of the issue. To this end, a licensee may issue more than one type of specified stablecoins under its licence. However, the licensee should discuss with the HKMA before issuance of an additional type of specified stablecoins, e.g. a specified stablecoin that references other currencies.

4.2.2. A licensee that wishes to issue an additional type of specified stablecoins should demonstrate to the HKMA that it has adequate capabilities and resources for managing the issuance of different types of specified stablecoins, and that the issuance of an additional type of specified stablecoins will not adversely impact its existing issuance activities.

4.3. Purpose and soundness of issue

4.3.1. Section 11 of Schedule 2 to the SO stipulates that the issue of a specified stablecoin by a licensee must be prudent and sound, having regard to the purpose, business model and operational arrangement of the issue. To this end, the licensee should:

(i) Adopt a strategy that aligns with the principle of ensuring the soundness and reliability of the specified stablecoins it issues;

(ii) Have in place a business plan that is realistic, concrete, viable, and has a reasonable prospect of generating sufficient demand for the specified stablecoins it issues to ensure sustainability of its licensed stablecoin activities;

(iii) Carry on licensed stablecoin activities in a prudent manner, for example to up-keep its reputation and to collaborate with reputable partners, such that it would not adversely affect the interests of specified stablecoin holders and/or monetary and financial stability of Hong Kong;

(iv) Comply with statutory and regulatory requirements in relevant jurisdictions; and

(v) Have adequate capability and resources to execute its business plan, and cope with internal and external shocks as well as unexpected contingencies.

4.3.2. When considering whether a licensee is carrying on licensed stablecoin activities with prudence and soundness, factors including but not limited to the following should be taken into account:

(i) The nature, complexity and scale of the business model and operational arrangement of the licensee;

(ii) The risks to the continuity of the financial functions provided or to be provided by the licensee;

(iii) The effect of any disruption to the continuous performance of such functions and activities that may have on the monetary and financial stability of Hong Kong; and

(iv) The mitigating measures that are implemented by the licensee.

5. Financial resources

5.1. Minimum paid-up share capital

5.1.1. Section 4 of Schedule 2 to the SO sets out the minimum criteria on financial resources of a licensee. A licensee should demonstrate that it has sufficient financial resources to maintain its licensed stablecoin activities and to meet all its obligations, as well as to ensure an orderly exit, either voluntarily or as a result of revocation of its licence. The licensee must maintain at all times a paid-up share capital of at least HK$25,000,000 (or an equivalent amount in another currency that is freely convertible into Hong Kong dollars) or other financial resources in an equivalent amount as approved by the Monetary Authority. Under section 17 of the SO, the Monetary Authority may attach to a licence any condition that the Monetary Authority considers appropriate, including but not limited to imposing requirements for the licensee to maintain additional financial resources, such as requiring a level of paid-up share capital greater than that set out in the minimum criteria applicable in relation to the licensee.

5.1.2. The proportion of a licensee's financial resources that are used to meet the financial resources requirement should only be used for the purposes of its business activities and should not be used for any dealing with its related companies or parties, including shareholders, directors and senior management.

5.1.3. The requirements in paragraphs 5.1.1 and 5.1.2 do not apply to a licensee that is an authorized institution. A licensee that is an authorized institution should comply with requirements under the Banking Ordinance (Cap. 155) and relevant guidance.

5.2. Liquid assets

5.2.1. Section 4 of Schedule 2 to the SO stipulates that a licensee must have adequate financial resources and liquid assets to meet its obligations as they will or may fall due. To this end, the licensee should maintain sufficient liquid net assets funded by equity (i.e. not from loans, guarantees or borrowings of similar nature) to meet its obligations. When considering the sufficiency of liquid net assets, factors including but not limited to the historical as well as projected operating expenses should be taken into account. To ensure fulfilment of such requirement, the licensee should ensure that there is secure ongoing source of financial resources.

5.2.2. The requirements in paragraph 5.2.1 do not apply to a licensee that is an authorized institution. A licensee that is an authorized institution should comply

with requirements under the Banking Ordinance (Cap. 155) and relevant guidance.

6. Risk management

6.1. Overview

6.1.1. Section 9 of Schedule 2 to the SO stipulates that a licensee must have in place and implement adequate and appropriate risk management policies and procedures for managing the risks arising from the carrying on of its licensed stablecoin activities that are commensurate with the scale and complexity of those activities.

6.2. Risk governance

6.2.1. Risk governance refers to the formal arrangements that enable the Board and senior management of a licensee to establish a sound business strategy, articulate and monitor adherence to risk appetite and risk limits, and identify, measure, manage and control risks.

6.2.2. To ensure effective risk management, a licensee should establish a set of risk governance arrangements, whereby the responsibilities of the Board, specialised committees (if any), senior management and different functions of the licensee, are well-defined.

6.2.3. In practice, a licensee should establish three lines of defence which are independent from one another in risk governance.

(i) The first line of defence is provided by business units, which should conduct risk identification, assessment, management and reporting on an ongoing basis.

(ii) The second line of defence is provided by independent risk management and compliance functions. The risk management function is responsible for the overall risk identification, assessment, monitoring, reporting, control and mitigation, while the compliance function is responsible for managing compliance risk (see paragraph 7.1.6).

(iii) The third line of defence should be provided by an independent internal audit function (see paragraph 7.1.7).

6.2.4. A licensee should ensure that its risk management, compliance and internal audit functions (collectively, the "internal control functions") have adequate authority and resources to perform their duties, clear responsibilities and accountability, as well as a direct reporting line to the senior management (for risk management and compliance functions) or the Board / a Board committee

(for internal audit function). In addition, the risk management function should have direct access to the Board, while the compliance function should have the right to report matters to the Board directly as necessary. The internal control functions should also be independent from front-line business units, and have unfettered access to information that is necessary for carrying out their duties.

6.3. Risk management framework and internal control system

6.3.1. A licensee should establish an effective risk management framework, with clearly defined and documented policies and procedures, for the identification, assessment, monitoring, reporting, control and mitigation of risks. The licensee's risk management policies and procedures should take into account all the activities performed by the licensee and cover all material risks, including but not limited to credit, liquidity and market risks (see paragraph 6.4), technology risks (see paragraph 6.5), operational risks (see paragraph 6.6), reputation risks (see paragraph 6.7), and money laundering and terrorist financing risks (see Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Stablecoin Issuers)).

6.3.2. For risk identification and assessment, a licensee should, on an ongoing basis, identify and assess its exposure to all material risks associated with its businesses. In the identification of risks, the licensee should take into account both external and internal factors, such as industry and market trends, any particular sectors that the licensee aims to serve, as well as its own business model and operations.

6.3.3. For risk monitoring and reporting, a licensee should implement measures to monitor its risk profiles and material exposures on an ongoing basis. The measures should include qualitative and quantitative assessments of the licensee's risk exposure, as well as appropriate metrics that provide an early warning on the materialisation of risks. The licensee should provide timely risk reports with comprehensive, accurate, actionable and comprehensible information to its senior management and the Board. The results of the risk monitoring, as well as other relevant materials, such as assessments of the risk management framework performed by the risk management function or internal audit function / external auditors, regulatory reports, and management letters issued by external auditors, should also be included in the reports.

6.3.4. For risk control and mitigation, a licensee should establish an effective internal control system that promotes efficient operation, provides reliable financial and management information, safeguards the availability, integrity and confidentiality of essential data, enables detection and prevention of irregularities, frauds and errors, ensures effective risk management systems and ensures compliance with relevant statutory provisions, regulatory requirements and internal policies. The internal control system should cover all material risks,

and include appropriate policies and procedures to control or mitigate the risks, processes for verifying compliance with internal controls, as well as consequences of non-compliance.

6.3.5. A licensee should review its risk management framework and internal control system regularly and at least on an annual basis. Any shortcomings identified during such review should be promptly addressed and reflected in the updated framework as well as policies and procedures. The framework, policies and key procedures, as well as any material changes, should be approved by the Board. The licensee should also conduct regular audits to assess (i) whether its operations are in compliance with its risk management framework and internal control system, as well as the applicable regulatory requirements, and (ii) whether the risk management framework and internal control system are adequate in addressing the material risks encountered by the licensee. The licensee should report the audit outcomes, including any material findings, to the HKMA in a timely manner and promptly provide the audit report and relevant supporting documents to the HKMA upon request.

6.4. Credit, liquidity and market risk management

6.4.1. Paragraph (a) of section 5(6) of Schedule 2 to the SO stipulates that a licensee must have in place and implement adequate and appropriate risk management policies and procedures for managing its reserve assets to ensure that they are properly managed so that valid redemption requests can be honoured without undue delay. To this end, the licensee's risk management framework should cover credit, liquidity and market risks. The licensee should ensure that the specified stablecoins it issues are fully backed by the reserve assets at all times, in both normal and stressed conditions, such that it is able to meet all valid redemption requests without undue delay.

6.4.2. For credit risk management, a licensee should implement measures to manage credit risk exposures to the counterparties in relation to the management of its reserve assets. Having regard to the creditworthiness of each counterparty, the licensee should set out and enforce internal limits on the credit risk exposures, which should be applied taking into account the linked counterparties. In practice, the licensee should establish and maintain a set of response procedures in the event that any of the internal limits have been exceeded, including prompt notification to the HKMA if any such internal limit has been exceeded for a prolonged period of time (e.g. more than one (1) business day). The licensee should also set out internal targets for facilitating the maintenance of credit risk exposures to counterparties within the boundaries of the internal limits.

6.4.3. For liquidity risk management, a licensee should establish an effective framework for projecting and monitoring liquidity demand arising from valid redemption requests under normal and stressed conditions. The licensee should

implement measures for managing the liquidity profile of the reserve assets (including intraday liquidity management), such as managing the allocation to the types of instruments, as well as maturities and counterparties, to ensure that the liquidity profile of its reserve assets would enable it to meet all valid redemption requests without undue delay. In formulating the policies and procedures, factors including but not limited to the liquidity of instruments, trading hours and settlement timeframes, term and early withdrawal option (for deposits) and risks of concentration should be taken into account.

6.4.4. A licensee should put in place liquidity risk indicators for monitoring the liquidity profile of the reserve assets, such as cash ratio and proportion of reserve assets that could be converted to cash for meeting redemption demand within certain timeframes. In practice, the licensee should set out and enforce internal limits for the liquidity risk indicators, as well as establish and maintain a set of response procedures in the event that any of the internal limits have been exceeded, including prompt notification to the HKMA if any such internal limit has been exceeded for a prolonged period of time (e.g. more than one (1) business day). The licensee should also set out internal targets for facilitating the maintenance of liquidity risk indicators within the boundaries of the internal limits.

6.4.5. For market risk management, a licensee should put in place market risk indicators for monitoring the market risk profile of the reserve assets. In practice, the licensee should set out and enforce internal limits for the market risk indicators, as well as establish and maintain a set of response procedures in the event that any of the internal limits have been exceeded, including prompt notification to the HKMA if any such internal limit has been exceeded for a prolonged period of time (e.g. more than one (1) business day). The licensee should also set out internal targets for facilitating the maintenance of market risk indicators within the boundaries of the internal limits. In addition, as a risk mitigating measure, the licensee should apply an appropriate degree of over-collateralisation for the reserve assets to provide sufficient buffer for potential changes in market prices, having regard to the market risk profile of the reserve assets.

Stress test

6.4.6. A licensee should conduct stress tests regularly based on severe but plausible scenarios to assess the robustness of its portfolio of reserve assets when facing credit, liquidity and market stress as well as adequacy of risk management measures. These scenarios, as well as the assumptions used in the scenarios, should be reviewed regularly, and any material changes should be approved by the Board.

6.4.7. A licensee should conduct stress tests on at least a quarterly basis, and should submit the methodologies, data sources and results of each stress test to the Board and the HKMA.

6.5. Technology risk management

6.5.1. A licensee should put in place a technology risk management framework to ensure (i) the adequacy of information technology ("IT") controls, (ii) the quality and security, including the reliability, robustness, stability and availability, of its technologies, and (iii) the safety and efficiency of its operations. Such framework should cover, but is not limited to, the following areas.

Token management

6.5.2. For each type of specified stablecoins it issues, a licensee should clearly document (i) the token standards used, (ii) the distributed ledgers on which such specified stablecoins are issued, and (iii) the architecture of all smart contracts (including token contract, proxy contract, multi-signature contracts, etc.) in respect of such specified stablecoins, including upgradeability (if any), state variables, functions, function modifiers, libraries, interfaces, etc.

6.5.3. A licensee should identify all operations in relation to the management of the full lifecycle of each type of specified stablecoins it issues, which should cover deploy, configure, mint, burn, upgrade, pause, resume, blacklist, remove blacklist, freeze, remove freeze, whitelist, usage of any operational wallets, etc. For each operation, the licensee should put in place a required level of authorisation proportionate to the level of risk of the operation, as well as triggers and conditions for execution. In addition, the licensee should ensure that high-risk operations are designed in a way that prevents any single party from being able to perform the relevant operations unilaterally (e.g. by multi-signature protocol). The licensee should also put in place detailed procedures with necessary controls to ensure that the execution of operations, including exception handling, is secure. Where applicable, the licensee should also impose additional security measures, such as setting velocity limits on transactions, restricting minting only to whitelisted wallet addresses, timelock on certain operations, pre-signed transactions for certain operations, off-chain simulation and checking of signed transactions before broadcasting transactions, etc. to minimise risks of being compromised.

6.5.4. A licensee should authorise suitable staff members to execute operations, and such staff members should go through appropriate screening and training. The execution of different operations should also be sufficiently segregated and split between different authorised staff members to ensure there are adequate checks

and balances and minimise the risk of any single point of failure or collusive manipulation. To ensure that operations can be carried out in a timely manner, the licensee should also put in place a staffing plan to ensure relevant personnel are available for the necessary execution of operations. Furthermore, procedures should also be put in place for the transition of the roles and responsibilities of, or changes to the authorised staff members, as well as for immediate revocation of an authorised staff member's authority. The licensee should also ensure there are sufficient checks and balances such that no authorised staff member should be able to have full control over role management (e.g. assigning roles of authorised personnel, altering the transaction approval processes, changing the number of required authorised staff members, etc.).

6.5.5. In respect of each type of specified stablecoins it issues, a licensee should identify the technological elements that would impact the issuance, redemption, as well as the usage of such specified stablecoins. In particular, for distributed ledgers on which the specified stablecoins are to be operated, the licensee should assess the robustness of the technologies, including but not limited to the security infrastructure, such as cryptography used; the consensus mechanism, encompassing factors like level of decentralisation, fault tolerance level and incentives mechanism; the capacity and scalability; the availability and results of third party audits or assessments; the resistance to common attacks, including a 51% attack or similar attacks which would have an impact on transaction finality; and the historical security track record, as well as risks relating to code defects, breaches, exploits and other threats. The licensee should also engage a qualified third party entity to audit (e.g. formal verification, security review) the smart contracts in respect of such specified stablecoins on at least an annual basis as well as whenever there is deployment, redeployment, or an upgrade to the smart contracts, to ensure that the smart contracts (i) are implemented correctly, (ii) consistent with the intended functionalities, and (iii) are, to a high level of confidence, not subject to any vulnerabilities or security flaws. When assessing whether a third party entity is qualified, factors including but not limited to its size, capabilities, expertise, track record, reputation, as well as presence in Hong Kong should be considered.

6.5.6. A licensee should implement measures for continuously monitoring the availability, capacity, performance, as well as expected updates or changes in the underlying technology, as well as for reporting any exceptions (e.g. failure or unavailability). Policies and procedures should also be put in place for responding to material changes or incidents (see paragraph 6.8).

Wallet and private key management

6.5.7. A licensee should put in place effective controls and procedures for private key management covering its full lifecycle, including but not limited to key

generation, distribution, storage, usage, back-up, recovery, destruction, etc. The licensee should identify all seeds and/or private keys relevant to the management of the specified stablecoins it issues, and adopt measures including but not limited to those listed below, on a scale proportionate to the significance of the seeds and/or private keys to its operations. Generally speaking, the seeds and/or private keys involved in (i) deployment or upgrade of smart contracts in relation to the specified stablecoins, (ii) role management (e.g. setting and revoking roles of minters and other roles that are involved in the management of the specified stablecoins), as well as (iii) operations that materially affect the supply of the specified stablecoins (e.g. large-scale minting and burning) ("Significant Seeds and/or Private Keys") should be subject to elevated security standards.

(i) Hardware and software management: A licensee should identify all hardware and software involved in wallet and private key management, including but not limited to storage media for the seeds and/or private keys, devices for interacting with the storage media of seeds and/or private keys, policy engines for managing authorisation for access to or usage of seeds and/or private keys, personal security devices, transmission devices, smart cards, signing applications and key management systems. The licensee should ensure that the hardware and software adopted are secure, reliable and effective, and that the procurement channels are secure with effective measures to minimise the risks of supply chain attack. In addition, the licensee should ensure that there are clearly defined responsibilities and effective measures for initialisation, usage, management, maintenance, and destruction / discontinuation of hardware and software. Responsible personnel should also undergo appropriate screening and training.

(ii) Key generation: A licensee should ensure the seeds (where applicable) are generated in a non-deterministic manner using strong and widely recognised cryptographic algorithms which ensures randomness and that the seeds are not reproducible. Private keys should be generated or derived from seeds in line with the above requirements. The key ceremony should be conducted by the licensee and only by a minimal number of authorised staff members with stringent controls in place to prevent leakage, as well as sufficient checks and balances. The seeds and/or private keys should be generated in a secure environment, such as a hardware security module ("HSM") with appropriate certification. For Significant Seeds and/or Private Keys, generation should occur offline and incorporate elevated security measures. In practice, the generation of such seeds and/or private keys should be conducted in an air-gapped environment, with effective physical security controls in place.

(iii) Key distribution: For the distribution of seeds and/or private keys, a licensee should adopt a secure methodology to ensure that the integrity and confidentiality of the seeds and/or private keys are safeguarded, for example via integrity mechanisms, physical security measures (for manual distribution) as well as encryption using strong and widely recognised cryptographic algorithms. Mechanisms should also be put in place for establishing assurance over the integrity and confidentiality of the seeds and/or private keys subsequent to their distribution, as well as for detecting any integrity failures or breaches of confidentiality.

(iv) Key storage: The seeds and/or private keys should be safeguarded in secure storage media, such as HSM with appropriate certification, in a secure facility with stringent access control and monitoring systems located in Hong Kong, or at a location acceptable to the HKMA. Other hardware or software for managing the usage of seeds and/or private keys should also be securely safeguarded in secure environments. Where multiple seeds and/or private keys are involved in the adoption of a multi-signature mechanism, the seeds and/or private keys should be stored separately in secure environments which are isolated from one another. The licensee should also ensure that the private keys are not displayed in the full alphanumeric form. For Significant Seeds and/or Private Keys, the licensee should ensure that the storage media, as well as other hardware or software for managing the usage of such seeds and/or private keys are safeguarded in an air-gapped environment, and that they are not stored in any computational environment or memory space in any systems connected to the Internet.

(v) Physical security of key storage: A licensee should ensure that the physical location and storage media are safeguarded against physical damage or unauthorised access, and monitoring measures are implemented to detect and respond to suspected unauthorised access. Examples of measures include (i) placing the storage media in rack cabinets placed in within a secure area safeguarded by mantrap as well as multiple layers of multi-factor authentication for access control, (ii) establishing alert and logging systems for access, (iii) implementing environmental control and monitoring measures (e.g. fire, temperature, electromagnetic fields), (iv) putting in place monitoring measures by closed-circuit television ("CCTV"), etc. In addition to storage media of seeds and/or private keys, other hardware involved in private key management should also be safeguarded within secure environments with necessary access control measures.

(vi) Key inventory: A licensee should maintain a key inventory with timely updates, which should include information about each private key (e.g. personnel authorised to access the private keys, function of private keys, status of the private keys, etc.) to facilitate its key management.

(vii) Key usage: A licensee should put in place effective policies and procedures for managing the usage of seeds and/or private keys. The allowed operations and conditions for key usage should be clearly set out and strictly enforced. Access to seeds and/or private keys should be tightly restricted among staff members who are authorised by the licensee and have undergone appropriate screening and training, and should be based on the principle of least privilege (i.e. access rights should be restricted to the greatest extent possible). Key usage should also be safeguarded by multi-factor authentication, and the private keys should be used within trusted environments. In addition, measures should be put in place to ensure (i) staff members responsible for key usage are able to interpret the semantic content of the transactions to be approved, and (ii) consistency between transactions to be approved and the semantic content displayed to staff members. Adequate security measures should also be implemented to minimise the risks of authorised staff members being compromised (e.g. kidnap and extortion). For Significant Seeds and/or Private Keys, key usage and the management of authorisation should require direct physical presence within the confines of the air-gapped environment where the storage media for seeds and/or private keys is safeguarded, and the transfer of transaction information between the air-gapped environment and other environment should be properly safeguarded to prevent tampering.

(viii) Key rotation and destruction: A licensee should identify seeds and/or private keys that are being frequently used and hence have a higher probability of leakage, and consider implementing measures for regular key rotation to minimise the risks of seeds and/or private keys being compromised. Also, the licensee should implement measures for the destruction of seeds and/or private keys where applicable and ensure that all copies of the seeds and/or private keys, including back-ups, are destroyed. Comprehensive impact analysis as well as verification should also be carried out prior to destruction of seeds and/or private keys.

(ix) Key compromise: A licensee should implement measures for monitoring usage of seeds and/or private keys (e.g. IP checking, behaviour monitoring, alert for key activities, device screening, on-chain monitoring, access control monitoring, etc.). The licensee should also implement measures to promptly address any actual or suspected compromise of the seeds and/or private keys. Upon detection of a compromise, the licensee should immediately notify the designated personnel to initiate an incident response and revoke (or destruct) the compromised seeds and/or private keys. Following the revocation, the process of generating and deploying new keys using secure methods should be carried out to ensure the ongoing security of token operations.

Measures should also be implemented for investigating the issue and carrying out any disciplinary actions for wilful or negligent mishandling.

(x) Key back-up: Tying in with its incident management framework and business continuity plan (see paragraph 6.8), a licensee should identify an appropriate scope of back-up of seeds and/or private keys. The licensee should ensure these seeds and/or private keys are backed-up in Hong Kong (or a location acceptable to the HKMA) at multiple secure locations, and the locations and nature of the back-up materials should be kept confidential from third parties. The licensee should also ensure that the seeds and/or private keys cannot be re-generated based solely on the back-ups stored in a single physical location. In addition, the back-ups should be generated and distributed with at least the same level of security standard for the original seeds and/or private keys. The licensee should utilise robust storage media for safeguarding the back-up, with measures for preventing unauthorised access as well as tamper-evident features. Any re-generation of seeds and/or private keys should require at least the same level of security as the business-as-usual key usage arrangement (e.g. re-generation would require the same number of quorum as key usage, with sufficient segregation of duties).

(xi) Key recovery: The licensee should put in place effective procedures for recovering seeds and/or private keys in a timely manner, whereby the conditions for triggering recovery procedures, authorisations required, procedures for key recovery, as well as validation actions for ensuring security of the re-generated keys are clearly documented and enforced. The authorisation control for key recovery should be at least as robust as the authorisation control for the usage of the original seeds and/or private keys. The recovery procedures should be regularly tested and rehearsed to ensure operational smoothness and assess its effectiveness. The licensee should put in place procedures to inform the HKMA in the event where key recovery procedures are triggered, as well as procedures to conduct reviews for identifying potential issues and enhancing measures after such procedures are triggered.

(xii) Logs: A licensee should maintain logs for the full lifecycle of seeds and/or private keys, covering key generation, distribution, storage, usage, back-up, recovery, revocation, destruction, as well as any access to them (including successful and failed attempts). The logs may include different types of logs (e.g. CCTV footage, access logs, on-chain transaction logs, internal system logs, etc.). Among other things, the logs should ensure that any access to the seeds and/or private keys can be traced to the relevant staff members. The licensee should clearly designate staff members to maintain the logs and define their responsibilities, and implement measures to ensure that the logs are retained for a sufficiently long period of time and are not subject to

unauthorised editing. The licensee should also review the logs periodically to ensure that all access to seeds and/or private keys are in line with the authorisations granted.

Account management

6.5.8. During the customer on-boarding process, a licensee should adopt an effective authentication method to establish and verify the identity of a potential customer having regard to the nature of the customer (i.e. natural or non-natural person). The licensee should also establish at least one secure ongoing communication channel with the customers. The licensee should inform its customers of such communication channels and that any message which purports to be sent by or on behalf of the licensee via any other means is not reliable.

6.5.9. When fulfilling a customer's request for issuance or redemption of the specified stablecoins it issues, a licensee should transfer funds only to and accept fund transfers from the customer's pre-registered bank accounts (or other types of pre-registered accounts, in case funding channels other than banks are used), as well as transfer specified stablecoins only to and accept transfers of specified stablecoins from the customer's pre-registered wallet addresses / accounts. The licensee should implement effective measures to ensure that only bank accounts (or other types of pre-registered accounts, in case funding channels other than banks are used) which are in the customer's name, and wallet addresses / accounts belonging to the customer / in the customer's name can be pre-registered with the licensee.

6.5.10. A licensee should authenticate customers' identities as customers perform account operations (e.g. logging into accounts, requesting for issuance or redemption of specified stablecoins, changing their particulars, pre-registering bank accounts or wallet addresses). The licensee should consider implementing an effective two-factor authentication mechanism in a manner proportionate to the risks of the account operations, where at least two out of the three types of factors (i.e. (i) something a customer knows; (ii) something a customer has; and (iii) something a customer is) are utilised for authentication. Where any information (e.g. one-time password ("OTP")) is being delivered in the authentication process, the licensee should ensure the information is delivered through a secure channel and in a secure manner. If device binding or registration is one of the authentication methods, the licensee should implement adequate measures (e.g. limiting the number of devices being bound or registered) to minimise the risks of compromise. If an OTP is used as an authentication factor, the licensee should implement effective management and security measures (e.g. implementing sound key management practice to safeguard the secret code for generating the OTP). In addition to two-factor authentication, a notification should also be sent to the customer via the secure communication channel in a timely manner. The licensee should implement

other measures, including but not limited to requirements on the strength (e.g. length, complexity and history) of passwords, reminder for changing passwords, limitations on the number of login or authentication attempts, timeout controls, time limits for authentication as well as validity of OTP (if adopted), to enhance account security.

6.5.11. A licensee should implement measures to ensure all transactions in relation to customers' accounts are logged, providing a clear audit trail. Secure mechanisms should be adopted for logging detailed transaction data such as transaction identifiers, timestamps and parameter changes, with strict access controls for authorised personnel only. The licensee should also offer avenues for customers to review their past transactions.

6.5.12. A licensee should also establish effective monitoring mechanisms to prevent, detect and block unauthorised access to customers' accounts and fraudulent transactions in relation to customers' accounts. Suspicious or high-risk transactions should be subject to specific screening and evaluation procedures. The licensee should also implement measures, including but not limited to allowing customers to set limits on different types of transactions, to minimise the risks of fraudulent transactions. In addition, the licensee should put in place procedures to monitor and manage the risks associated with fraudulent emails, websites, apps, etc. The licensee should also provide advice to its customers on security precautions as appropriate.

6.5.13. If a licensee provides programmable access for customers to their accounts (e.g. via an application programming interface), the licensee should implement adequate security measures for such channels, covering authentication, integrity, confidentiality and authorisation. The licensee should also provide relevant detailed documentation to customers.

Security management

6.5.14. A licensee should implement adequate measures to maintain a high level of security of its IT assets, which should include the following:

(i) System security: A licensee should put in place and maintain control procedures and baseline security requirements to safeguard its IT assets. A licensee should also have a process to ensure all configurations and settings of its IT assets are adequately and accurately maintained. Internal reviews on the compliance of the security settings with the baseline security requirements, as well as vulnerability assessments for detecting security vulnerabilities should be performed regularly.

(ii) Authentication and access control: A licensee should enforce restricted access to its IT assets through robust authentication mechanisms and

defined access control rules, which specify allowable user interactions with application functions, system resources, and data. Users should be uniquely identified using unique user-identification codes (e.g. user identifiers) coupled with secure authentication methods (e.g. passwords) to ensure traceability of actions. The licensee should also implement stringent password policies that prevent the use of simple passwords and mandate regular updates, particularly for high-risk activities which should employ multi-factor authentication. The management of privileged and emergency access should be handled with extra diligence, requiring strict authorisation protocols, formal approval processes, continuous monitoring of activities, secure storage and timely modification of access credentials. User access re-certification as well as rotation of access credentials should be performed on a periodic basis as well. A security administration function should be established and a set of procedures should be put in place for administering the allocation of access rights to IT assets. In addition, proper segregation of duties within the security administration function or other compensating controls (e.g. peer reviews) should be implemented to mitigate the risks of unauthorised activities being performed by the security administration function.

(iii) Security monitoring: A licensee should implement adequate and effective measures as well as necessary tools (e.g. intrusion prevention system, intrusion detection system, endpoint detection and response technology, security information and event management solutions) for continuous security monitoring, covering areas including log retention, monitoring of critical configurations and security settings to identify unauthorised changes, blocking anomalies on IT assets, performing real-time analysis on security logs and events for critical IT assets, handling of suspicious and confirmed breaches or cyber incidents, etc. Measures should also be implemented to ensure relevant personnel are notified upon the detection of suspected breaches.

(iv) Patch management: A licensee should implement a patch management process covering the identification, categorisation, prioritisation and installation of security patches. The process should include the assessment of severity and impact on systems to ensure that security patches for its IT assets are deployed in a timely manner.

(v) Physical and personnel security: A licensee should implement adequate physical security measures for safeguarding its IT assets. Critical information processing facilities should be housed in secure areas such as data centres and network equipment rooms with adequate security controls on physical access. Access to these areas should be restricted to authorised personnel only, with the access rights being subject to regular review and updates. If third party personnel (e.g. service

providers) require access to such areas, approval should be obtained and their activities should be monitored. The licensee should also implement environmental controls to monitor and mitigate risks associated with environmental hazards, power failures and electrical disturbances. The licensee should perform periodic risk assessments for such secure areas to identify security threats and operational weaknesses, and to assess the adequacy of safeguarding controls. For sensitive technology-related positions, appropriate background checks and screening should be conducted.

(vi) Endpoint security and end-user computing: A licensee should implement adequate measures to restrict unauthorised activities at the endpoint devices (including devices provided by the licensee and any other devices that can access the licensee's computer resources). The licensee should also implement controls to detect and prevent attacks (e.g. computer viruses and other malicious software) on endpoint devices. If the licensee's computer resources can be accessed using mobile devices, controls should be put in place to manage the risks of working in an unprotected environment (e.g. approval process for the use of mobile devices accessing the licensee's computer resources, authentication control, data encryption). If the licensee adopts end-user computing, it should implement adequate measures to address the associated risks, covering areas including data security, documentation, data / file storage and back-up, system recovery, audit responsibilities and training. The licensee should also maintain an inventory of end-user developed software.

Information management

6.5.15. A licensee should put in place policies and procedures for information management, which should cover the following areas:

(i) Information ownership and classification: A licensee should put in place procedures for assigning information owner and classifying information into different categories according to the degree of sensitivity with corresponding protection measures, which should include access and authentication control to ensure access to information is restricted to authorised persons.

(ii) Information in storage and transmission: A licensee should ensure sensitive information is encrypted and stored in a secure environment with strong and widely recognised encryption techniques so that it is protected from theft and unauthorised access or modification. Sensitive information that is being transmitted to and/or from the licensee's

systems should also be secured by end-to-end encryption, using strong and widely recognised encryption techniques.

(iii) Information retention and disposal: A licensee should ensure that the information it collects and maintains in the course of its business is on a need-to-have basis, and that access to information is on a need-to-know basis. In addition, a licensee should implement an information retention and disposal policy to limit the amount of information stored and the retention period of information, taking into account legal, regulatory and business requirements. Procedures should also be in place for secure deletion of information that is no longer needed.

IT services and operations

6.5.16. A licensee should put in place appropriate policies and procedures to ensure the delivery of effective IT services and operations, which should cover the following areas:

(i) IT operations management and support: A licensee should establish an IT function for the delivery of day-to-day technology services and support to business units. The management of the IT function should formulate an internal service level agreement with business units to specify system availability, performance requirements, capacity for growth, and the level of support provided to users. Policies and procedures should also be put in place by the IT function to manage the delivery of agreed support and services. Detailed operational instructions such as computer operator tasks, as well as job scheduling and execution, as well as the procedures for on-site and off-site back-up of data and software (e.g. frequency, scope, retention periods of back-up, and frequency of restoration tests) should be documented clearly.

(ii) Incident and problem management: As part of its incident management framework (see paragraph 6.8), a licensee should establish an IT incident management framework to handle IT incidents where the resolution timeframe is commensurate with the severity level of the incident, as well as an IT problem management process to identify, classify, prioritise and address all IT problems in a timely manner. The IT problem management process should set out clear roles and responsibilities of staff involved, and include regular trend analyses of past incidents to facilitate identification and prevention of similar problems.

(iii) Performance monitoring and capacity planning: Processes should be put in place to ensure that the availability, capacity and performance of its IT assets is continuously monitored and exceptions are reported in a

timely manner. A licensee should also implement proper capacity planning taking into account planned business activities. Capacity planning should also be extended to cover back-up systems and facilities in addition to the production environment.

(iv) IT facilities and equipment maintenance: To ensure the reliability, robustness, stability and availability of its IT assets and back-ups, a licensee should maintain its IT assets and back-ups in accordance with industry practice and suppliers' recommended service intervals and specifications. IT assets that are critical to the continuity of IT services should be identified and single points of failure should be minimised. An IT asset inventory should be maintained to keep track of all hardware and software purchased and leased.

Project and change management

6.5.17. A licensee should establish an effective framework for managing technology-related projects.

(i) Project life cycle: A licensee should establish a framework for the management of major technology-related projects (such as any in-house software development), setting out, among other things the project management methodology applied. The licensee should adopt a full project life cycle methodology governing the process of planning, development, implementation and maintenance of projects. The methodology should clearly allocate responsibilities and set out deliverables at each phase, as well as define security requirements at an early stage for each project. The licensee should establish guidelines and standards for software development and programme coding with reference to industry practice. Where a project involves the acquisition of external software packages, the licensee should implement adequate measures to address the risks arising from the use of such packages (e.g. breach of software licence agreement or patent infringement, security risks), as well as to ensure that ongoing maintenance and adequate support for software packages are available through written contracts established with vendors.

(ii) Testing and acceptance: The licensee should establish a formal testing and acceptance process to ensure that only properly tested and approved systems are deployed to the production environment. The process should cover areas including but not limited to business logic, security controls and system performance under various stress-load scenarios and recovery conditions. In addition, the licensee should appoint an independent third party to conduct quality assurance reviews of major technology-related projects with the necessary assistance from the legal

and compliance functions, as well as conduct penetration testing to identify any weaknesses. As part of a quality assurance review, the licensee should implement source code reviews (e.g. peer review and automated analysis review) to identify and address vulnerabilities and non-compliance with its internal policies, control requirements, regulations and applicable laws.

(iii) Segregation of duties and systems: A licensee should ensure that the development, testing and production environments are segregated, and that there is a proper segregation of duties so that only authorised personnel can access the development, testing and production library and environments. The licensee should also ensure that production data is not used in development or testing unless the data has been desensitised and approval has been obtained from the information owner. In addition, vendors' access to the development or testing environments, if any, should also be closely monitored.

(iv) Change management: A licensee should implement a proper and effective change management process covering the process of planning, scheduling, applying, distributing and tracking changes to its IT assets. The process should be able to capture all changes, and should include elements including but not limited to obtainment of approval; classification and prioritisation; determination of impact; roles and responsibilities of each relevant party; programme version controls; scheduling, tracking, monitoring and implementation; rolling back changes upon the emergence of issues; post implementation verification; and audit trails. Procedures should also be put in place to manage emergency changes, which should include approval processes, as well as processes to seek endorsement where changes need to be implemented as a matter of urgency and approval seeking is impracticable.

Network management

6.5.18. A licensee should implement network management and security measures to ensure the robustness of its networks.

(i) Network management: A licensee should assign responsibility for network management to personnel with relevant expertise. The standards, design, diagrams and operating procedures should be clearly documented, kept up-to-date, communicated to relevant staff members, and reviewed periodically. Communications facilities that are critical to the continuity of network services should be identified, and single points of failure should be minimised by the automatic re-routing of communications through alternate routes should critical nodes or links

fail. Measures should be implemented to monitor the network on a continuous basis to reduce the likelihood of network traffic overload and detect network intrusions.

(ii) Network security: A licensee should put in place procedures regarding the use of networks and network services, covering the available networks and network services, authorisation procedures for access to networks and network services, as well as controls and procedures to protect access to network access points, network connections and network services. The licensee should establish a secure network infrastructure (covering the design of Demilitarised Zone as well as configuration of network servers, intrusion detection system, firewalls and routers) to protect critical systems. Reviews should be conducted regularly on the security parameter settings of network devices such as routers, firewalls and network servers to ensure that they remain current. In addition, the licensee should segregate internal networks to different segments having regard to the access control needed for the data stored in, or systems connected to, each segment. Encryption technology and network monitoring tools covering internal and external networks should be put in place to protect sensitive information in internal networks, communication channels to third parties and external networks. Measures should be implemented to detect and block actual and attempted network intrusion, and network operational personnel should be alerted on a real-time basis of potential security breaches. Audit trails of activities in critical network devices should be maintained and reviewed regularly.

Cybersecurity

6.5.19. A licensee should implement adequate measures for identifying cyber risks and threats in respect of the licensee in a timely manner, and deploy effective measures to defend against cyberattacks.

(i) Risk identification and assessment: A licensee should implement risk assessment measures to identify and classify cybersecurity risks stemming from its operations, including but not limited to its internal operations, external connection with other parties, etc. The licensee should also put in place procedures for identifying assets, activities and processes that warrant additional cybersecurity controls. In addition, the licensee should conduct periodic cyber risk assessments covering relevant and important IT assets, with the scope of assessment being able to cater for both widely known and emerging risks, as well as update its cybersecurity controls from time to time.

(ii) Threat intelligence: A licensee should put in place adequate measures for monitoring threat intelligence to discover emerging threats. The threat intelligence should be analysed such that mitigating measures can be implemented in a timely manner. The licensee should also provide cybersecurity awareness training as well as reminders, based on latest threat intelligence, to its staff members regularly.

(iii) Vulnerability detection: A licensee should implement processes for detecting vulnerabilities against cyberattacks. Antivirus and anti-malware tools should be used to detect attacks and protect the licensee's IT assets from malware. Regular cybersecurity assessments, including vulnerability scanning, penetration testing and intelligence-led cyberattack simulation testing should be conducted in a manner which is commensurate with the licensee's cybersecurity risk profile to detect control gaps in employee behaviours, security defences, policies and resources. The results of the testing should be used to assess the adequacy of the licensee's cybersecurity controls, and appropriate actions should be taken to mitigate the issues, threats and vulnerabilities in a timely manner.

(iv) Cyber incident response: As part of its incident management framework and business continuity plan (see paragraph 6.8), a licensee should implement measures for detecting cyber incidents, as well as put in place incident response procedures to set out the procedures on responding to cyber incidents. The incident response procedures should include procedures for timely actions to limit or contain the impact of cyber incidents, and restore its operations according to the recovery strategies and recovery time objectives. Escalation and communication processes should be put in place so that the incidents are reported and communicated to relevant stakeholders in a timely manner. Processes should also be put in place such that digital forensic evidence of cyber incidents are recorded, analysed and investigated, and that mitigating measures are implemented to prevent similar incidents.

Disaster recovery

6.5.20. As part of its incident management framework and business continuity plan (see paragraph 6.8), a licensee should develop an IT disaster recovery plan to ensure that critical IT assets and services can be resumed in accordance with the business recovery requirements.

Management of technology service providers

6.5.21. A licensee should take into account the guidance on third party risk management (see paragraph 6.6.2 to 6.6.11) when managing technology service providers.

6.5.22. In addition to the general third party risk management measures, when engaging with technology service providers, a licensee should ensure its service providers have adequate resources and expertise to adhere to the licensee's technology risk management policies. Critical technology services should only be outsourced after a detailed assessment in line with relevant internationally recognised certification standards has been conducted on the prospective service provider's IT controls by an independent third party with satisfactory results. The assessment results should be shared with the HKMA. Outsourcing agreements should clearly define performance standards, hardware and software ownership, and include provisions for subcontracting (if any), ensuring the original service provider remains accountable for all services. The licensee should, to the extent appropriate and practicable, diversify its service providers to mitigate risks associated with single-provider dependencies and put in place comprehensive contingency plans for critical technology services which are provided by technology service providers.

6.6. Operational risk management

6.6.1. A licensee should put in place effective policies and procedures to manage its operational risks. The licensee should conduct risk identification and assessments regularly, to identify the material operational risks associated with its business activities, processes and systems, which include but are not limited to theft, fraud and misappropriation of reserve assets, business disruption, etc. To this end, the licensee should draw reference from operational incidents occurring in relevant sectors. For each identified risk, the licensee should adopt an appropriate method for assessing such risk, including estimating the probability that such risk will materialise taking into account the causes of such risk and assessing their potential impact to the licensee's business activities, processes and systems.

Third party risk management

6.6.2. A licensee should put in place policies on managing the risks associated with third party arrangements. In practice, before entering into a third party arrangement, the licensee should identify and assess the risks that may arise from such arrangements and their materiality to the licensee's business activities, processes and systems, and implement measures to adequately address the material risks. In particular, the licensee should assess the importance and criticality of the services or operations to be performed by the third party entities, identify the reasons and the needs for such arrangement, as well as the impact on the licensee's risk profile.

6.6.3. A licensee should assess the risks of disruption in the third party entities' operations, and as part of its incident management framework and business continuity plan (see paragraph 6.8), implement contingency arrangements maintained by both the third party entities and the licensee itself to ensure the impact on the licensee's operations is minimised. The licensee should also identify feasible and viable alternative arrangements so that the impact of any prolonged disruption can be minimised. The licensee remains solely responsible for meeting its regulatory obligations under the SO and other relevant regulatory requirements prescribed by the HKMA from time to time.

6.6.4. A licensee should perform appropriate due diligence on the prospective third party entity, including conducting thorough testing, to ensure that the services or operations performed by the third party entities will meet the performance standards and/or expectations, and are compliant with the applicable regulatory requirements. Aspects to be included as part of the due diligence should include the cost factor, quality of services or operations, financial soundness, reputation, managerial skills, technical and operational capabilities, availability of third party audits, assessments or compliance certifications, capacity to meet the licensee's demand on an ongoing basis, familiarity with the industry, capacity to keep pace with innovation in the market, etc.

6.6.5. For third party arrangements, a licensee should enter into written contractual agreements with the relevant third party entities, which sets out (i) the type and level of services or operations as well as performance standards, (ii) operational arrangements including any subcontracting arrangements, (iii) contingency arrangements, (iv) rights and obligations of the licensee and the third party entities including termination rights as well as the fees and charges payable by the licensee, (v) rights of the licensee to access, retrieve and retain accurate and up-to-date records in Hong Kong on a timely basis and ability to make those records available for inspection by relevant authorities and the licensee's internal and external auditors (if applicable), (vi) data handling controls such as data storage, back-up, protection, confidentiality and removal arrangements upon termination or expiry of the contract (if applicable).

6.6.6. On an ongoing basis, the licensee should implement measures for continuous monitoring of the operational status of the third party entities and the availability of the services or operations they perform, as well as for identifying and reporting any disruptions. The licensee should also regularly conduct risk assessments to ensure all material risks arising from the third party arrangements are adequately addressed, and regularly perform quality review to ensure that the performance of the third party entities is up to standard or meets expectations and take appropriate actions to rectify any deficiencies. In addition, the licensee should regularly review the third party arrangements to assess whether they should be renegotiated or renewed, with reference to the current market standards and its business requirements. The contingency arrangements

put in place by the third party entities and the licensee itself should also be regularly reviewed and tested.

6.6.7. A licensee should ensure that access to data relevant to the licensee by relevant authorities (including the HKMA) as well as the licensee's internal and external auditors, is not impeded by the third party arrangements. The licensee should also ensure that measures are in place to facilitate on-site examinations and off-site reviews of the operations of the third party entities (insofar as the relevant operations are related to the licensee's business) both announced and unannounced, by authorised parties including the HKMA and the licensee's internal and external auditors.

6.6.8. A licensee should implement measures to ensure that the third party arrangements comply with the Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486) and relevant codes of practice, guidelines and best practices issued by the Office of the Privacy Commissioner for Personal Data.

6.6.9. A licensee should also ensure that only authorised employees of the third party entities are able to access data related to the licensee's operations on a need-to-know basis. The licensee should ensure that in the event of termination or expiry of a third party arrangement, any data received by the relevant third party entity which is related to specified stablecoin holders and/or customers of the licensee is either returned to the licensee or destroyed by the relevant third party entity.

6.6.10. If a third party arrangement involves the provision of services by entities outside Hong Kong, a licensee should assess the additional risks that may arise from such arrangement taking into account factors such as the governing law of the third party agreement with third party entities. These include but are not limited to ensuring right of access to data relevant to the licensee for examination by relevant authorities including the HKMA, and the licensee's internal and external auditors (see paragraph 6.6.7). The licensee should also assess the level of access by authorities in the relevant jurisdiction outside Hong Kong to any data which relates to the licensee, and implement measures to ensure that the licensee promptly notifies the HKMA in the event that such authorities seek access to such data.

6.6.11. A licensee should have in place policies for assessing the materiality of third party arrangements and prompt notification to the HKMA of any material third party arrangements prior to the commencement of such arrangements, as well as procedures for continuously monitoring existing non-material third party arrangements and notifying the HKMA if such arrangements become material over time. Material third party arrangements include but are not limited to custody for reserve assets, distribution of specified stablecoins, critical IT services, etc.

6.7. Reputation risk management

6.7.1. A licensee should implement effective processes for the management of reputation risks that is appropriate for the size and complexity of its business. The licensee should (i) identify and assess the potential reputation implications of its activities (including its licensed stablecoin activities), (ii) implement a monitoring and reporting mechanism to keep track of such risks as well as events that may lead to materialisation of such risks, (iii) take proactive actions to minimise the identified risks, and (iv) respond swiftly to mitigate any impact should such risks materialise. The licensee should also implement measures for notifying the HKMA of any incidents that may have a material adverse effect on its reputation.

6.7.2. In particular, a licensee should, on a best efforts basis, implement adequate measures for identifying and handling potential fraud cases that may be associated with its business (including specified stablecoins it issues). Examples include impersonation of the licensee for conducting activities that may breach relevant laws and regulations. Furthermore, the licensee should also monitor any activities and incidents that may be viewed as being associated with itself and may therefore impact its reputation. Examples include wrapping of the specified stablecoins issued by the licensee, which may lead specified stablecoin holders and/or potential specified stablecoin holders into believing that such wrapped tokens are issued by the licensee. To address the associated risks, the licensee should implement appropriate measures on monitoring (e.g. monitoring websites, social media posts, etc.), and put in place measures for handling these cases, which include but are not limited to issuing reminders to the public, reporting to the relevant authorities, engagement with media agencies, etc.

6.8. Incident management, business continuity and exit

Overview

6.8.1. A licensee should establish an effective governance arrangement for the development, maintenance and implementation of a comprehensive incident management framework as well as business continuity and exit plans, which should include clear lines of responsibilities, an effective and efficient escalation procedure, detailed procedures for the triggering and execution of incident response procedures, business continuity recovery strategies or business exit plan, as well as a clear communication strategy to relevant stakeholders including specified stablecoin holders.

Incident management

6.8.2. A licensee should establish an effective incident management framework to ensure a timely response to incidents which have or may have a material adverse effect on its business, operations, assets or reputation, and/or result in the breach or potential breach of any statutory or regulatory requirements by the licensee or its Board, senior management or staff members. The connection between the incident management framework and the licensee's business continuity plan and disaster recovery plan (see paragraph 6.5.20) should be clearly documented.

6.8.3. In practice, a licensee should set out the criteria for classifying the materiality and severity of incidents, and establish effective arrangements for detecting, monitoring and evaluating incidents. The licensee should also establish a set of indicators that may signal the need for the activation of response procedures. The indicators should cover areas including but not limited to the following.

(i) Credit, liquidity and market risks (e.g. failure of counterparty; surge in redemption demands; prolonged exceeding (e.g. more than one (1) business day) of internal limits on credit risk exposures to counterparties (see paragraph 6.4.2), liquidity risk indicators (see paragraph 6.4.3), market risk indicators (see paragraph 6.4.5), etc.)

(ii) Technology risks (e.g. failure in IT assets; IT security breaches; exploits of smart contracts; incidents associated with distributed ledgers such as hard and soft forks, serious network congestion, outage, attacks and irrecoverable failure; loss of access to private keys; unauthorised access to private keys; cyber incidents, etc.)

(iii) Operational risks including third party risks (e.g. disruption of key operations; prolonged absence of key personnel; operational disruption or failure of third party entities; negative media coverage on third party entities, etc.)

(iv) De-pegging risks (e.g. material deviation of secondary prices from par; anomalies in order book depth and bid-ask spread in secondary markets; concentrated specified stablecoins holdings in certain specified stablecoin holders, etc.)

(v) Reputation risks (e.g. negative media coverage; impersonation fraud; spreading of rumours, etc.)

(vi) Compliance and legal risks (e.g. breach of statutory and regulatory requirements by the licensee or its staff members; potential litigation, etc.)

6.8.4. A licensee should put in place response procedures for containing the impact of incidents. Among other things, a licensee should put in place strategies for

coping with liquidity stress or other incidents that could potentially cause the licensee to fail to maintain a full backing of reserve assets or meet all valid redemption requests without undue delay.

6.8.5. A licensee should implement measures for ensuring the orderly issuance, redemption and distribution of specified stablecoins in the event that the licensee's normal operations are disrupted. If the licensee engages third party entities for the distribution of specified stablecoins it issues, it should also put in place measures for dealing with potential disruption to the services provided by such third party entities. Such measures may include identifying multiple alternative third party entities, etc.

6.8.6. A licensee should also implement measures for addressing material de-peg of specified stablecoin in secondary markets, such as enhancing communications with the public and specified stablecoin holders, increasing the frequency of disclosure of reserve assets, maintaining additional redemption channels, etc. Among other things, a licensee should take into account factors including the mismatch between business hours when redemption requests are being processed, as well as the round-the-clock operations of the specified stablecoins.

6.8.7. A licensee should implement measures for addressing failures in the underlying technological elements of the specified stablecoins it issues. Among other things, the licensee should maintain robust back-up records with corresponding procedures for facilitating recovery, or in the event of irrecoverable failure of the distributed ledgers, for facilitating the redemption of such specified stablecoins.

6.8.8. As part of the incident management process, a licensee should collect and preserve forensic evidence as appropriate to facilitate subsequent investigation and prosecution of offenders if necessary. After the incident, the licensee should also perform a review to identify the root causes and adopt rectification actions as necessary.

Business continuity management

6.8.9. Section 16(1) of Schedule 2 to the SO stipulates that a licensee must have in place and implement adequate and appropriate systems of control for appropriate planning to support timely recovery and continuity of critical functions in relation to its licensed stablecoin activities when there is an occurrence of significant operational disruption. A licensee should put in place an effective business continuity management programme with adequate resources to ensure the preservation of essential data, as well as the continuation and timely recovery of critical functions in relation to its licensed stablecoin activities in the event of disruption, and such programme should include a business continuity plan. Senior management should have sufficient oversight

of the licensee's business continuity management programme and offer necessary support to staff members to ensure the effective implementation of the business continuity plan.

6.8.10. A licensee should establish formally documented business continuity plan to provide comprehensive guidance and procedures for managing business disruptions, and enabling the resumption and continuation of critical operations, with the ultimate goal of returning to normal business operations. The plan should outline critical operations and key dependencies, both internal and external, the criteria for activating the business continuity plan, and integrate elements such as business impact analyses, recovery strategies, escalation and communication procedures, and contact details of key personnel. Copies of the business continuity plan should be stored at locations separate from the licensee's primary sites. Senior management and key personnel should be provided with a summary of key steps to take in case of an emergency.

6.8.11. In practice, a licensee should put in place processes for conducting business impact analyses on a regular basis to identify critical business operations, services and internal support functions which have to be continuously and effectively delivered in the event of a disruption. The licensee should also identify potential stress scenarios that may disrupt its services, and put in place a monitoring mechanism as well as a set of indicators that may signal the need for the activation of recovery strategies.

6.8.12. Among other things, a licensee should identify the minimum level of critical services that needs to be maintained in the event of a disruption, and develop realistic, measurable and achievable recovery objectives, including a maximum tolerable downtime to recover and resume the minimum level of critical services, a recovery time objective to recover critical IT resources and a recovery point objective to recover data.

6.8.13. A licensee should put in place a range of recovery strategies as well as key steps, milestones and processes for execution to address the potential disruption to its businesses. When formulating the strategies and procedures, the licensee should assess the impact, timeframe for implementation, probable success of the recovery strategies as well as the associated risks. The recovery priorities should be guided by the results of the business impact analyses. The licensee should also take into account situations where more than one kind of disruption occurs simultaneously, and ensure that the measures it implements would be able to address multiple disruptions at once.

6.8.14. To ensure the effectiveness of the business continuity plan, a licensee should identify key information that is critical to its business (including its licensed stablecoin activities) and back up such information as soon as possible and on an ongoing basis at an off-site location. For certain information, the licensee should also consider implementing instantaneous back-up (e.g. real-time

mirroring technology) to ensure high availability of records. The licensee should implement measures for retrieving the back-up information when necessary. Such measures as well as the detailed procedures should be documented in the business continuity plan.

6.8.15. A licensee should select alternate sites for business and IT recovery, which should be sufficiently distanced from the primary site. The alternate sites should be readily accessible and available for occupancy within the timeframe required in the licensee's business continuity plan. The alternate sites for IT recovery should have sufficient IT equipment to meet the recovery strategies as set out in the licensee's business continuity plan.

6.8.16. A licensee should avoid placing excessive reliance on third party entities for business continuity plan support. If vital recovery services (e.g. provision of alternate sites) are provided by third party entities, the licensee should manage the risks associated with such services accordingly (see paragraphs 6.6.2 to 6.6.11), and specify the type and capacity of support, as well as the required lead-time in the written contractual agreements with the third party entities.

Business exit plan

6.8.17. Section 16(2) of Schedule 2 to the SO stipulates that a licensee must have in place and implement adequate and appropriate systems of control to ensure that (i) an orderly wind-down of its licensed stablecoin activities could be implemented, and (ii) redemption of specified stablecoins issued by the licensee could be honoured in an orderly manner. A licensee should put in place a business exit plan for the orderly wind-down of its licensed stablecoin activities should other options be proven not possible. The business exit plan should cover a range of scenarios which may render an orderly wind-down necessary, as well as measures for monitoring any materialisation or potential materialisation of such scenarios. The licensee should also set out detailed procedures to be taken upon a triggering of the business exit plan, which should include but are not limited to processes for (i) liquidating reserve assets under normal and stressed conditions (including measures for ensuring maximisation of proceeds from the liquidation of reserve assets and minimisation of impact on the overall market stability), (ii) facilitating specified stablecoin holders to file redemption claims, (iii) distributing proceeds to specified stablecoin holders, and (iv) making arrangements for operations involving third party entities. The licensee should assess the time and resources required for the execution of the business exit plan, and implement measures to ensure sufficient time and resources are available in case of a need for orderly wind-down. The licensee should also assess the legal certainty and operational feasibility of the procedures.

Review, testing and reporting

6.8.18. A licensee should review its incident management framework, as well as the business continuity and exit plans regularly and at least on an annual basis, and whenever there has been an activation of the incident response procedures or business continuity recovery strategies. Any shortcomings identified during such review should be promptly addressed and reflected in the updated framework and plans. The framework and plans, as well as any material changes, should be approved by the Board. The licensee should also conduct regular audits to assess (i) whether the execution of incident response procedures and/or business continuity recovery strategies (if any) are in compliance with its framework and plans, as well as the applicable regulatory requirements, and (ii) whether the framework and plans are realistic and remain current. The licensee should report the audit outcomes, including any material findings, to the HKMA in a timely manner and promptly provide the audit report and relevant supporting documents to the HKMA upon request.

6.8.19. A licensee should ensure the incident management framework, as well as the business continuity and exit plans are subject to regular testing (including simulation exercise), at least on an annual basis, to ensure that all relevant personnel are familiar with the framework and plans and their responsibilities thereunder, and are able to take prompt actions accordingly. The result of each testing should be reported to the Board and senior management, and the licensee should ensure that the framework and plans are updated to address any shortcomings which are identified during the testing.

6.8.20. A licensee should submit to the HKMA the contact details of key personnel involved in the implementation of the incident management framework, as well as the business continuity and exit plans, and should promptly notify the HKMA of any changes to such key personnel. The licensee should also put in place procedures for notifying the HKMA in a timely manner of the materialisation, or anticipated materialisation, of any scenarios under which the licensee's incident response procedures, business continuity recovery strategies or business exit plan are or are likely to be triggered.

6.8.21. If a licensee's incident response procedures, business continuity recovery strategies or business exit plan involve the delay of redemption of specified stablecoins issued by the licensee (i.e. redemption requests will not be fulfilled within the one (1)-business day requirement), the licensee should implement measures to seek the Monetary Authority's written consent before implementing such delay.

7. Corporate governance

7.1. Corporate governance

7.1.1. Section 9 of Schedule 2 to the SO stipulates that a licensee must have in place and implement adequate and appropriate risk management policies and procedures for managing the risks arising from the carrying on of its licensed stablecoin activities that are commensurate with the scale and complexity of those activities. To this end, a licensee should establish a sound governance arrangement for the purpose of effective decision making and proper management of risks arising from the carrying on of its licensed stablecoin activities. Such arrangement should include, among others, a clear organisational structure with well-defined, transparent and clearly documented allocation of responsibility. There should also be clear documentation on decision making procedures, reporting lines, internal reporting and communication processes.

Board of directors

7.1.2. A licensee's Board has the ultimate responsibility for the operations and soundness of the licensee. The Board should clearly define and document its responsibilities, authorities, composition requirements, as well as arrangements of its own work (including appointment of directors, Board members' qualification and training, Board performance evaluation, governance in group structures (if applicable), communication with the HKMA, etc.). The Board should have an adequate number and appropriate composition of members to ensure sufficient checks and balances and collective expertise for effective and objective decision-making.

7.1.3. Generally, at least one-third of the Board members should be independent non-executive directors ("INEDs") so as to ensure sufficient checks and balances, bring in outside experience and provide objective judgement. Prior to each appointment of a director, including an INED, a licensee should submit to the HKMA its reasons and justifications for such intended appointment. The requirement in this paragraph does not apply to a licensee that is an authorized institution, which should comply with requirements under the Banking Ordinance (Cap. 155) and relevant guidance.

7.1.4. The responsibilities of the Board should include but are not limited to:

(i) Setting and overseeing the objectives of the licensee and strategies for achieving such objectives;

(ii) Overseeing the establishment of a corporate structure with well-defined, transparent and clearly documented allocation of responsibilities as well as internal reporting and communication processes;

(iii) Delegating and appointing appropriate members of the Board to chair and/or serve as members on different specialised committees (e.g. remuneration committee, audit committee), which are responsible for formulating policies in their respective areas;

(iv) Appointing and overseeing the licensee's senior management to ensure that they exercise their duties in accordance with approved policies and delegated authorities;

(v) Establishing and overseeing risk governance and approving risk management policies and key procedures, as well as ensuring effective internal control functions; and

(vi) Setting the corporate values and standards of the licensee as well as overseeing its remuneration policy.

Senior management

7.1.5. The Board should work closely with senior management of the licensee, who are accountable to the Board. Senior management includes (i) a licensee's chief executives and where the licensee is an authorized institution, the stablecoin manager, and (ii) other senior executives, which primarily consist of managers (see paragraphs 7.2.6 to 7.2.7). The Board should clearly set out the responsibilities, accountability mechanisms and reporting lines of senior management, as well as ensure that there are effective arrangements to assess their performance and hold them accountable. The responsibilities of senior management should include but are not limited to:

(i) Proposing business plans for deliberation and approval by the Board, implementing the strategies approved by the Board, and attending Board committee meetings where appropriate;

(ii) Establishing a corporate structure with well-defined, transparent and clearly documented allocation of responsibilities as well as internal reporting and communication processes;

(iii) Ensuring the competency of the licensee's staff members by establishing an effective staff recruitment, appraisal and development programme;

(iv) Establishing an effective risk management framework, including implementing risk management policies and procedures as approved by the Board, as well as ensuring effective internal control functions; and

(v) Establishing an effective management information system that provides the Board and senior management with regular and accurate information.

Compliance and internal audit functions

7.1.6. A licensee should establish and maintain a compliance function, which should assist the licensee to ensure compliance with relevant statutory provisions, regulatory requirements and codes of conduct. The compliance function should have a direct reporting line to senior management, as well as the right to report matters to the Board directly. The compliance function should establish compliance policies and guidelines to set out its organisation and responsibilities, as well as measures to manage compliance risk, so as to ensure that compliance risk is adequately and effectively managed. The compliance policy, as well as any material changes, should be approved by the Board and subject to regular review as well as additional review if the circumstances so warrant.

7.1.7. A licensee should establish and maintain an internal audit function. The internal audit function should be responsible for conducting objective and impartial assessments to evaluate the effectiveness of the licensee's internal systems of control, identify weaknesses and recommend enhancements. It should report directly to the Board or a Board committee, and have in place a structured process for audit planning, performance of audit procedures and reporting. An audit charter should be put in place to set out the organisation, authorities, responsibilities, objectives and scope of work of the internal audit function. The audit charter, as well as any material changes, should be approved by the Board and subject to regular review as well as additional review if the circumstances so warrant.

7.1.8. The compliance and internal audit functions should have (i) clearly defined responsibilities and accountability, (ii) sufficient authority and standing, (iii) professional competence, and (iv) adequate resources to perform their duties. They should also be independent from front-line business units, and have unfettered access to information that is necessary for carrying out their duties.

7.1.9. The compliance function and internal audit functions should be independent and not be substituted by one another. If a licensee relies on external or group service, the licensee should demonstrate to the satisfaction of the HKMA the effectiveness of the alternative arrangements.

Corporate governance measures

7.1.10. As part of a sound governance arrangement, a licensee should establish a code of conduct for its directors, senior management and staff members which sets out the standards of integrity and probity expected of them, and incorporates the requirements for the fitness and propriety of its chief executives, directors, managers, and where the licensee is an authorized institution, the stablecoin manager. The code of conduct should also provide examples of acceptable and unacceptable behaviour, and should explicitly prohibit any behaviour that could lead to non-compliance by the licensee with its obligations under the SO or result in unaddressed conflicts of interest. In addition, the code of conduct should cover the requirements under the Prevention of Bribery Ordinance (Cap. 201). The licensee should implement adequate measures to ensure that the code of conduct is fully understood by all directors, senior management and staff members and is properly enforced.

7.1.11. As stipulated in section 13(3) of Schedule 2 to the SO, a licensee must have in place and implement adequate and appropriate risk management policies and procedures to identify, prevent, manage and disclose potential and actual conflicts of interest between itself and specified stablecoin holders. To this end, the licensee should implement adequate measures to prevent or manage such conflicts. Measures that could be implemented include but are not limited to adopting segregation of duties, establishing information barriers, disallowing directors or staff members from benefiting from the improper use of confidential information or advantages offered to them which may lead to unfair, improper or illegal behaviour, preventing directors or staff members with outside activities from having inappropriate influence within the licensee in respect of matters which have some connection with, or touch upon, their outside activities.

7.1.12. A licensee should have a remuneration policy that is in line with its business strategies and long-term interest. The Board should oversee the establishment and the implementation of the remuneration policy, including being responsible for approving the remuneration packages of the chief executives (and the stablecoin manager where the licensee is an authorized institution) and heads of internal control functions. The remuneration and performance measures of the staff members of the internal control functions should be determined independently of those of the front-line business units such that the independence of staff members of the internal control functions is not compromised.

7.2. Fitness and propriety

7.2.1. Sections 7 and 8 of Schedule 2 to the SO sets out the minimum criteria in relation to fitness and propriety as well as knowledge and experience. When considering whether a person is fit and proper to hold relevant position and whether a person possesses the relevant knowledge and experience, the

standards may vary depending on the exact position as well as responsibilities held by the person concerned.

Chief executives, stablecoin manager and directors

7.2.2. Section 7(2) of Schedule 2 to the SO stipulates that each person who holds the position of, among others, chief executive, director or stablecoin manager of a licensee must be a fit and proper person to hold the position. When considering whether a person is fit and proper to hold such positions, factors including but not limited to the following should be taken into account:

(i) The person's reputation and character: Whether the person has a relevant criminal record (e.g. convictions for fraud or other dishonesty, contravention of any provision of legislation designed to protect members of the public against financial losses due to dishonesty, incompetence or malpractice); whether the person has been involved in any business practices that appear to be deceitful, oppressive, or otherwise improper, or which otherwise reflect discredit on the person's method of conducting business;

(ii) The person's knowledge and experience, competence, soundness of judgment and diligence: Whether the person has had experience of similar responsibilities, and the person's record in fulfilling them; where appropriate, whether the person has had appropriate qualifications and training; whether the person has a sound degree of balance, rationality and maturity demonstrated in the person's conduct and decision-making;

(iii) The person's records of non-compliance: Whether the person has any record of non-compliance with various non-statutory codes, or has been reprimanded, disciplined or disqualified by regulators or professional bodies in Hong Kong or elsewhere;

(iv) The person's record as a controller, director, chief executive and stablecoin manager: Whether the person has been a controller, director, chief executive, stablecoin manager, or is otherwise concerned in the management, of any body corporate, partnership, unincorporated institution that has been censured, disciplined, publicly criticised, investigated or whose licence, registration or authorisation has been revoked by any regulator in Hong Kong or elsewhere, or has been wound up or adjudicated insolvent by a court in Hong Kong or elsewhere; whether the person has been disqualified by a court in Hong Kong or elsewhere from being a director of a company. In these cases, factors such as the seriousness of circumstances leading to the winding up or investigation, the extent of the person's involvement, the lapse of time and the person's conduct since should be taken into account;

(v) The person's business record and other business interests, and the person's financial soundness and strength: Whether the person has any business interests and/or adverse financial position that would undermine the prudence and soundness of the issue of specified stablecoins by the licensee, and/or the confidence of specified stablecoin holders;

(vi) The person's interests in the company: Whether the person, in the case of an INED, has direct or indirect financial or other interests in the business of the licensee as well as the person's relationship, if any, with significant shareholders of the licensee; and

(vii) The person's time and commitment to the company: Whether the person, in the case of having outside mandates, is able to devote sufficient time and attention to perform the person's role; whether there are any potential conflicts of interest arising from such outside work.

7.2.3. In addition, pursuant to sections 53(2) and 58(1) of the SO, a licensee that is not an authorized institution must not appoint a person as the chief executive, and a person must not become a director of such a licensee, without the Monetary Authority's consent. Pursuant to section 66(2) of the SO, a licensee that is an authorized institution must not appoint a person as the stablecoin manager without the Monetary Authority's consent.

Controllers

7.2.4. Section 7(2) of Schedule 2 to the SO stipulates that each person who holds the position of, among others, controller of a licensee must be a fit and proper person to hold the position. When considering whether a person is fit and proper to hold such position, in addition to those set out in paragraph 7.2.2, factors including whether there could be conflicts of interest arising from the influence of a person holding the position of controller on the licensee, as well as the willingness and ability of the person to work collaboratively with other controllers and the senior management should also be considered. These factors for consideration should be taken into account in a manner proportionate to (i) the influence the person has, or is likely to have, on the conduct of the affairs of the licensee, and (ii) the potential impact of a person holding the position as controller on the interests of specified stablecoin holders and potential specified stablecoin holders.

7.2.5. In addition, a person must not become a controller of a licensee unless the person becomes such a controller in the circumstances set out in section 37(1) of the SO. Section 7(1) of Schedule 2 to the SO also stipulates that the licensee must have in place and implement adequate and appropriate systems of control

to ensure that the Monetary Authority is kept informed of the identity of each controller of a licensee. To this end, the licensee should put in place measures for keeping track of the identity of its controllers, as well as for seeking consent from the Monetary Authority in accordance with section 38 of the SO.

Managers

7.2.6. Section 7(3) of Schedule 2 to the SO stipulates that a licensee must have in place and implement adequate appropriate systems of control to ensure that each person who holds the position of manager of the licensee is a fit and proper person to hold the position. To this end, the licensee should:

(i) Clearly define the responsibilities of, and the skills, knowledge and experience required for, individual managerial positions, supported by up-to-date job descriptions, organisation charts and levels of authority;

(ii) Have in place a set of proper procedures for selecting and appointing managers and for satisfying itself regarding the fitness and propriety of candidates for managerial positions at the time of appointment or recruitment. In assessing the fitness and propriety of a manager or a prospective manager, factors set out in paragraph 7.2.2 should be taken into account, with due regard to the position that the person holds or is to hold;

(iii) Have in place effective and clearly defined systems for appraising the performance of managers, where such systems should not give undue weight to financial performance (e.g. achievement of profitability or market share) but should also have regard to other factors such as compliance with policies and procedures and regulatory requirements;

(iv) Have in place clearly defined policies and procedures for investigating breaches of policies and procedures or regulatory requirements by managers, or complaints about the conduct of managers, and for taking disciplinary actions where appropriate;

(v) Have in place clearly defined systems for taking action in respect of, and if necessary replacing, managers whose performance is assessed as unsatisfactory;

(vi) Ensure that managerial vacancies are filled promptly and that there are clearly defined arrangements to provide cover in the case of temporary vacancies;

(vii) Provide adequate training to managers; and

(viii) Ensure that the systems of control in relation to the appointment of managers are subject to periodic review by its internal audit function.

7.2.7. In addition, pursuant to section 63 of the SO, a licensee must notify the Monetary Authority within 14 days after the date on which a person (i) is appointed as a manager of the licensee, (ii) ceases to be a manager of the licensee, or (iii) is appointed as a manager for any specified affairs in addition to, or in place of, any existing specified affairs. Such notification must include the date on which the event occurred, and particulars of the concerned specified affairs.

8. Business practices and conduct

8.1. Information and accounting systems

8.1.1. A licensee should establish effective information and accounting systems to (i) record all business activities in a timely and accurate manner, including both on-chain and off-chain information, (ii) provide quality management information to enable effective and efficient management of business and operations, and (iii) maintain appropriate audit trails to demonstrate effectiveness of controls. A licensee should also properly maintain books and accounts and prepare financial statements and returns in compliance with all applicable regulatory reporting requirements and accounting standards. Sufficient back-up facilities and disaster recovery arrangements for the information and accounting systems should also be put in place.

8.1.2. A licensee should put in place adequate record keeping policies and systems for maintaining accurate and sufficient records of its books, accounts, management decisions and business activities, including both on-chain and off-chain information. The records should be maintained for a sufficiently long period, taking into account relevant statutory and regulatory requirements.

8.1.3. If the information and accounting systems of a licensee are located outside Hong Kong, the licensee should establish effective arrangements to ensure access to the systems, as well as to enable on-site examinations or off-site reviews, whether announced or not, by authorised parties including the HKMA.

8.2. Disclosure and reporting

8.2.1. When fulfilling its disclosure and reporting obligations, a licensee should ensure its information is accurate to the best of its knowledge, and is up-to-date and reflecting the actual operations of its businesses.

8.2.2. Among other things, as stipulated in sections 5(7) and 6(5) of Schedule 2 to the SO, a licensee should make adequate and timely disclosure to the public on matters in relation to reserve assets management and redemption. To this end, a licensee should fulfil its ongoing disclosure and reporting obligations as set out in paragraphs 2.7 and 3.6.

8.2.3. As regards the requirement in section 13(1) of Schedule 2 to the SO to publish a white paper in respect of each type of specified stablecoins issued by a licensee, the licensee should publicly disclose its white paper at a reasonably prominent location on its website. The licensee should notify the HKMA before it publishes or makes material changes to the white paper. The whitepaper should

be, where feasible, be composed in non-technical language that is easily comprehensible to the public.

8.2.4. For each type of specified stablecoins it issues, a licensee should set out in a white paper information including but not limited to:

(i) General information about the licensee;

(ii) Detailed information about the specified stablecoins;

(iii) Reserve assets management arrangement, as well as relevant arrangements with third party entities (if any);

(iv) Issuance, redemption and distribution mechanisms, covering the procedures, redemption rights, timeframe, any applicable conditions and fees involved, as well as arrangements with third party entities for distribution of the specified stablecoins (if any);

(v) Underlying technology of the specified stablecoins; and

(vi) Risks associated with using the specified stablecoins.

8.2.5. A licensee should submit to the HKMA on an annual basis its audited financial statements prepared in accordance with the applicable accounting standards, which should cover the reserve assets backing the specified stablecoins it issues. The audited financial statements should be submitted to the HKMA within four months of the financial year-end.

8.3. Personal data protection

8.3.1. A licensee should implement effective measures to ensure that it complies with the PDPO and relevant codes of practice, guidelines and best practices issued by the Office of the Privacy Commissioner for Personal Data.

8.4. Complaints handling

8.4.1. Section 14 of Schedule 2 to the SO sets out the minimum criteria regarding complaints handling and redress mechanisms. A licensee should ensure that the specified stablecoin holders have access to complaints handling and redress mechanisms that are adequate, accessible, affordable, independent, fair, accountable, timely and efficient.

8.4.2. A licensee should establish proper governance arrangements and segregation of duties, such that complaints will be handled by competent staff members who are not involved in the subject matter. The licensee should also have appropriate and effective policies and procedures in place for handling complaints, covering acknowledgement, investigation, escalation, remediation, resolution, responses and closing, as well as for following up issues of concern as identified during the complaints handling process. The licensee should also maintain sufficient records for an appropriate time period (i.e. at least two (2) years from the date of receipt of complaints, while being compliant with requirements on personal data protection), ensure confidentiality of information, as well as remedy the issues revealed by the complaints. In addition, the licensee should provide appropriate feedback and notification to the HKMA, upon the HKMA's request or in case of complaints that reveal compliance issues or repeated complaints on the same unaddressed matter. The licensee should make the complaints handling system accessible to the public. The licensee should disclose its complaints handling processes and expected timeframe at a reasonably prominent location on its website.

8.4.3. On the timeframe for handling complaints, a licensee should acknowledge a complaint within seven (7) calendar days of its receipt, providing the contact details of responsible staff member, as well as details of the complaints handling procedures. Within 30 calendar days after receiving a complaint, the licensee should provide the complainant with a full response, or an interim response explaining why the licensee is not in a position to make a response, as well as providing reasons for the delay and an indicative timeframe for a full response (generally not exceeding 60 calendar days). If the licensee is able to resolve a complaint or provide a response within seven (7) calendar days of receiving a complaint, it may combine the acknowledgement of the complaint with the response.

8.4.4. Where a licensee has entered into arrangements with third party entities for distribution of specified stablecoins it issues, it should put in place procedures to facilitate the handling by such third party entities of related complaints.

9. Glossary

Terms that are defined in the SO have their defined meaning when used in this Guideline. Other terms should be interpreted with reference to the definitions set out below where applicable.

Air-gapped environment	A computing environment in which all IT assets and networks are physically and logically isolated from external IT assets and networks (including the Internet)
Bank	Bank as defined in section 2(1) of part 1 of the Banking (Capital) Rules (Cap. 155L)
Business day	A day other than (i) a Saturday, (ii) a day which is a general holiday as specified in the General Holidays Ordinance (Cap. 149), or (iii) a gale warning day or a black rainstorm warning day as defined in section 71(2) of the Interpretation and General Clauses Ordinance (Cap. 1)
Distribution	The arrangement where a licensee engages a third party entity where the latter (i) provides channels for acquisition or disposal of specified stablecoins issued by the licensee (e.g. offering of specified stablecoins by broker-dealers, listing of specified stablecoins on exchange platforms), or (ii) provides liquidity on secondary markets as a business for specified stablecoins issued by the licensee
End-user computing	The transfer of information processing and system development capabilities from centralised data centres onto the user's desktop
Government	Sovereign as defined in section 2(1) of Part 1 of Banking (Liquidity) Rules (Cap. 155Q)
Independent non-executive director	A director who does not perform any executive functions within a licensee's organisation and is not under any undue influence, internal or external, political or arising through the incidents of ownership or otherwise, that would impede his exercise of independent and objective judgement
Information owner	An individual who has been assigned as the business owner of an application system and is accountable for the protection of information processed by, and stored in, this application system

Issuance	In relation to a specified stablecoin issued by a licensee, the process in which a licensee issues the specified stablecoin to a customer following a valid request
IT assets	Hardware, software, data, and systems maintained by a licensee (or via third party arrangements) for facilitating its IT operations
Key ceremony	A procedure for generating a unique pair of public and private keys
Licensed bank	Bank as defined in section 2(1) of the Banking Ordinance (Cap. 155)
Linked counterparties	In relation to a counterparty of a licensee ("reference counterparty"), another counterparty of the licensee that falls under the following categories: (i) Entities that control the reference counterparty or are controlled by the reference counterparty; (ii) Entities that are controlled by an entity that controls the reference counterparty; (iii) Entities that are economically dependent on the reference counterparty or an entity specified in item (i) or (ii); (iv) Entities that control and are economically dependent on an entity specified in item (iii) or are controlled by an entity specified in item (iii)
Mint	The creation of specified stablecoins on distributed ledgers
Multilateral development bank	Multilateral development bank as defined in section 2(1) of the Banking Ordinance (Cap. 155)
Outsource	A category of third party arrangement where a licensee uses a service provider to perform services that would otherwise be undertaken by the licensee itself
Public sector entity	Public sector entity as defined in section 2(1) of the Banking (Capital) Rules (Cap. 155L)
Public sector entity bank	PSE bank as defined in section 1(1) of Part 1 of Schedule 2 to the Banking (Liquidity) Rules (Cap. 155Q)
Qualified international organisations	Relevant international organizations as defined in section 2(1) of the Banking (Capital Rules) (Cap. 155L)

Redemption	In relation to a specified stablecoin issued by a licensee, the process in which a specified stablecoin holder receives from a licensee the par value of the specified stablecoin in the referenced currencies to which such specified stablecoin is referenced
Specialised committee	Committee established by the licensee to oversee specific areas of risk or governance, including but not limited to Board committees and management committees
Specified stablecoin holder	In relation to a specified stablecoin issued by a licensee, a person who holds the specified stablecoins
Third party arrangement	An arrangement that constitutes one of the following: (i) A provision of service to a licensee by a service provider (whether or not it is an intra-group entity); or (ii) An engagement of a third party for carrying out certain activities in relation to the licensed stablecoin activities of a licensee
Third party entity	An entity or a service provider that is involved in a third party arrangement