BANK OF MAURITIUS

Guideline for Virtual Asset related Activities

Month 2022

Page intentionally left blank

TABLE OF CONTENTS

Page intentionally left blank

INTRODUCTION

Background

The Virtual Asset and Initial Token Offering Services Act 2021 ("VAITOS Act"), which came into force on 7 February 2022, sets out a comprehensive legislative framework to regulate the business activities of virtual assets service providers and initial token offerings.

Section 8(3) of the VAITOS Act provides that a bank may, with the written approval of the Bank of Mauritius, apply:

(i) for a class "R" licence (Virtual Asset Custodian) or class "I" licence (Virtual Asset Advisory Services) to carry out the business activities of a virtual asset service provider; and

(ii) through its subsidiary, for a class "M" licence (Virtual Asset Broker-Dealer), class "O" licence (Virtual Asset Wallet Services) or class "S" licence (Virtual Asset Market Place) to carry out the business activities of a virtual asset service provider.

In addition to the above, banks may provide services to virtual asset service providers, issuers of initial token offering and to customers dealing in virtual assets. Bank may also have direct/indirect exposures to virtual assets, virtual assets service providers and issuers of initial token offering.

Purpose

This guideline sets out the principles to be followed by banks involved in activities related to virtual assets. The guideline is based on the principles set out in the second consultative document of the Basel Committee on Banking Supervision on the prudential treatment of cryptoasset exposures.

Authority

The Guideline is issued under the authority of section 50 of the Bank of Mauritius Act 2004 and section 100 of the Banking Act 2004.

Scope of application

The Guideline shall apply to all banks licensed under the Banking Act 2004 engaged in virtual asset related activities.

Effective date

The Guideline shall come into effect on xx month 2022.

Interpretation

"Act" means the Banking Act 2004;

"Bank" means the Bank of Mauritius established under Bank of Mauritius Act 2004;

"bank" has the same meaning as in the Banking Act 2004;

"banking services" refer to services provided by a bank under the Act;

"board" means the board of directors of a bank except for branches of foreign banks where board means the local advisory board/committee. For branches of foreign banks with no local advisory board, the responsibilities assigned to the board shall rest on the Chief Executive Officer of the branch;

"FSC" means the Financial Services Commission, Mauritius established under the Financial Services Act 2007;

"initial token offerings" or "ITO" means an offer for sale to the public, by an issuer of initial token offerings, of a virtual token in exchange for fiat currency or another virtual asset;

"issuer of initial token offerings" means a company registered as such under section 25(5) of the VAITOS Act;

"VAITOS Act" means the Virtual Asset and Initial Token Offering Services Act 2021;

"virtual asset", for the purpose of this guideline, are digital representations of value that may be digitally traded or transferred, and may be used for payment or investment purposes but does not include a digital representation of fiat currencies. Virtual assets include dematerialised securities (securities that have been moved from physical certificates to electronic book-keeping) that are issued through Distributed Ledger Technologies or similar technologies and are referred to as tokenised traditional assets. Dematerialised securities that use electronic versions of traditional registers and databases which are centrally administered are not deemed as virtual assets for the purpose of this guideline;

"virtual asset exchange" means a centralised or decentralised virtual platform, whether in Mauritius or in another jurisdiction –

a. which facilitates the exchange of virtual assets for fiat currency or other virtual assets on behalf of third parties for a fee, a commission, a spread or other benefit; and

b. which – (i) holds custody, or controls virtual asset, on behalf of its clients to facilitate an exchange; or (ii) purchases virtual assets from a seller when transactions or bids and offers are matched in order to sell them to a buyer, and includes its owner or operator but does not include a platform that only provides a forum where sellers and buyers may post bids and offers and a forum where the parties trade in a separate platform or in a peer-to-peer manner;

"virtual asset related activities" refer to activities involving virtual assets, including but not limited to:

i. activities falling under the scope of virtual asset service providers and issuer of initial token offerings;

ii. provision of services to virtual asset service providers, issuers of initial token offering and to customers dealing in virtual assets;

iii. direct and indirect exposure to virtual assets through:

   a. investments and trading in virtual assets;

   b. credit exposures guaranteed by virtual assets;

   c. credit exposures to or guaranteed by virtual asset service providers and issuers of initial token offerings; and

   d. credit exposures to or guaranteed by counterparties who have significant exposures to virtual asset providers, issuers of initial token offerings and significant dealings in virtual assets and

iv. investments in subsidiaries or other entities having significant dealings in virtual assets;

"virtual asset service provider" means a person that, as a business, conducts one or more of the following activities or operations for, or on behalf of, another person –

a. exchange between virtual assets and fiat currencies ***(Virtual Asset Broker-Dealer)***;

b. exchange between one or more forms of virtual assets ***(Virtual Asset Broker-Dealer)***;

c. transfer of virtual assets ***(Virtual Asset Wallet Services)***;

d. safekeeping of virtual assets or instruments enabling control over virtual assets ***(Virtual Asset Custodian)***;

e. administration of virtual assets or instruments enabling control over virtual assets ***(Virtual Asset Custodian)***; and

f. participation in, and provision of, financial services related to – (i) an issuer's offer and sale of a virtual asset; (ii) an issuer's offer or sale of a virtual asset ***(Virtual Asset Advisory Services)***;

"virtual asset wallet services" means the provision of a software application or other mechanism or medium to enable a person to transfer virtual assets; and

"virtual token" means any cryptographically secured digital representation of a set of rights, including smart contracts, provided on a digital platform and issued or to be issued by an issuer of initial token offerings.

1. Responsibilities of Board

1.1. The board shall:

i. ensure that the governance, risk management and assurance frameworks incorporate the risks associated with the virtual asset related activities;

ii. approve and periodically review the strategy, risk appetite, risk limits, risk management framework and relevant policies for virtual asset related activities;

iii. ensure that the board, senior management and other relevant staff have appropriate expertise and experience and are provided with relevant training for an effective understanding and oversight of the virtual asset related activities;

iv. set the roles and responsibilities of senior management, the internal governance and risk management structures with clear accountabilities for the management of the risks related to virtual asset related activities;

v. establish the approval procedures and delegation authorities for activities related to virtual assets; and

vi. receive timely and relevant risk reports on virtual asset related activities at least on a quarterly basis for an effective oversight.

2. Responsibilities of Senior Management

2.1. The senior management of banks shall:

i. establish the relevant systems, policies and procedures for implementing the board approved policy and strategy for virtual asset related activities;

ii. ensure that the risk management framework across the three lines of defence adequately addresses the associated risks and include relevant policies and procedures for an effective identification, measurement, monitoring, mitigation and management of risks associated to virtual asset related activities;

iii. ensure that the associated risks are closely monitored and that the board is kept informed through regular reporting;

iv. establish appropriate information systems that allow them to identify, aggregate, report and monitor all types of direct and indirect exposures to virtual assets;

v. ensure compliance with applicable legal and regulatory requirements, locally and overseas;

vi. regularly review the effectiveness of the framework, policies, tools and controls; and

vii. implement relevant internal structures with adequate resources, skills and expertise for managing the risks associated with virtual asset related activities.

3. Regulatory Approval

3.1. Banks shall seek the written approval of the Bank prior to:

i. applying for a class "R" licence (Virtual Asset Custodian) or class "I" licence (Virtual Asset Advisory Services) with the FSC to carry out the business activities of a virtual asset service provider;

ii. applying, through its subsidiary, for a class "M" licence (Virtual Asset Broker-Dealer), class "O" licence (Virtual Asset Wallet Services) or class "S" licence (Virtual Asset Market Place) with the FSC to carry out the business activities of a virtual asset service provider;

iii. making investments, under sections 30(1)(b)(iv) or 30(7) of the Act, in tokenised shares where these tokenised shares confer the same legal rights as ownership of the traditional (non-tokenised) version of those shares; and

iv. classifying virtual assets as Groups 1a and 1b Virtual Assets as set out in section 5.

3.2. The application for approval under sections 3.1(i) and 3.1 (ii) shall be accompanied by the risk assessment report of the bank covering the identified risks, potential impact, mitigating controls and the approval received from the board or the delegated authority of the board.

3.3. The application for approval under section 3.1(iv) shall be accompanied by the risk assessment reports of the bank and demonstrate how the virtual assets meet the criteria set out in the ***Annex***. Banks shall also provide an independent legal opinion confirming compliance with the criteria.

3.4. The Bank shall be informed whenever banks propose to take any exposure in virtual assets which do not qualify as Group 1a and 1b Virtual assets. The request shall include the risk assessment conducted covering the identified risks, potential impact and mitigating measures, the approval received from the board or delegated authority of the board, the risk appetite and risk limits, and the proposed treatment with respect to measurement of the risk and computation of the risk weighted assets and capital/liquidity requirements.

3.5. The approval of the Bank is not required for

i. the provision of banking services to virtual asset service providers, issuers of initial token offering and customers dealing in virtual asset service providers/issuers of

initial token offering. This includes the processing of payment transactions in respect of purchase, sale and redemption of virtual assets in exchange of fiat currencies; and

ii. investment and trading in virtual assets other than those:

a. covered under section 3.1 (iii); and

b. made on behalf of customers of the bank.

4. Risk Management Framework

4.1. Banks should establish policies and procedures to identify, assess and mitigate the risks (including credit risk, liquidity risk, market risk, operational risk, money laundering and terrorism financing and proliferation risks) related to virtual asset related activities on an ongoing basis.

4.2. Banks shall ensure that the risks associated with virtual asset related activities are duly addressed within their existing risk management framework, strategy, risk appetite policies and procedures for relevant prudential risks.

4.3. Prior to engaging in any virtual asset related activity, banks shall:

i. ensure that the strategy, risk appetite, risk limits and risk management framework, including relevant policies, are duly approved by the board;

ii. undertake a prudent and comprehensive risk assessment to ensure that the associated credit risk, liquidity risk, market risk, operational risk, money laundering/terrorism financing and proliferation risks and any other risk that may arise are duly identified, assessed, understood and mitigated;

iii. ensure that all relevant policies, procedures and processes are duly updated;

iv. implement relevant risk limits considering, inter alia, the potential impact of the volatility of the value of the virtual assets, the default of issuers/ redeemers or virtual assets and other relevant counterparties and cyber/ technology risk incidents;

v. clearly assign the responsibility for the management of the identified risks; and

vi. satisfy themselves that the virtual asset related activities are duly licensed and regulated.

4.4. Banks shall implement an appropriate risk monitoring process for exposures to virtual assets and other activities against the set strategy, risk appetite and risk limits.

Credit Risk

4.5.1. Banks may be exposed to credit risk through, inter alia, holdings of virtual assets, direct and indirect credit exposures to virtual asset service providers, issuers of initial token offerings or customers highly engaged in or exposed to virtual assets.

4.5.2. Banks shall ensure that the credit risk assessment takes into consideration the risks associated with virtual assets and that there are appropriate systems in place to monitor the value of virtual assets provided as collateral.

4.5.3. Banks shall satisfy themselves of their ability to take possession of and redeem the virtual assets provided as collateral and seek relevant legal opinions on the legal enforceability of their rights.

4.5.4. Banks shall ensure that the virtual assets recognised as collateral can be liquidated promptly.

4.5.5. Banks shall establish exposure limits for their holdings in virtual assets, their direct and indirect exposures to issuers/redeemers of the virtual assets and other relevant counterparties and their exposures to entities/customers engaged in activities related to virtual assets.

Liquidity Risk

4.5.6. Banks shall assess the potential impact of exposures to virtual assets on their liquidity position and factor such exposures into their internal liquidity adequacy assessment processes, where relevant. This shall, inter alia, include the ability to convert the virtual assets into fiat currency and the ability to redeem the virtual assets.

Market Risk

4.5.7. Banks shall ensure that their internal policies and procedures for the management of market risks take into consideration the potential losses from the volatility of the price of virtual assets.

4.5.8. Banks shall ensure that there are relevant systems for the monitoring of the price and for the valuation of the virtual assets.

Operational Risk and Cyber and Technology Risk

4.5.9. Banks shall ensure that their internal operational risk and cyber and technology risk management frameworks duly cover the risks associated with activities related to virtual assets, including but not limited to:

i. virtual asset related technology risks inherent to the supporting technology, including those used by third parties such as those relating to the stability of the Distributed Ledger Technology or similar technology network, validating design of the Distributed Ledger Technology, service accessibility, trustworthiness of the node operators and operator diversity;

ii. cyber and technology risks such as cryptographic key theft, compromise of login credentials and distributed denial-of-service attacks; and

iii. legal risks, including but not limited to potential fines due to the underpayment of taxes, failure to comply with tax reporting obligations, inability of banks to take possession of virtual assets provided as collateral in the event of default/margin call and inadequate disclosure to customers.

Money Laundering and Terrorism Financing and Proliferation Risk

4.5.10. Banks shall, pursuant to section 17 of the FIAMLA, identify, assess and understand the money laundering, terrorism financing and proliferation financing risks that may arise from virtual asset related activities and take appropriate measures to manage and mitigate these risks. Banks must document the risk assessment(s) in writing, keep it up to date and, on request, make it available to the Bank or any other relevant competent authorities without delay.

4.5.11. Banks shall ensure that their internal policies, controls and procedures, including those relating to customer due diligence and ongoing monitoring, are in place to mitigate and manage effectively the risks of money laundering, terrorism financing and proliferation financing associated with the virtual asset related activities. Banks must also regularly review, update and, where necessary, enhance their internal policies, controls and procedures.

4.5.12. Banks shall apply the risk-based approach as set out in the Guideline on Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation when providing any services to virtual asset service providers or to customers involved in virtual asset related activities, or when engaging in virtual asset related activities themselves or through their subsidiaries.

4.5.13. Banks shall ensure compliance with the relevant guidelines and instructions issued by the Bank in their dealings with virtual asset service providers or other virtual assets related activities.

5. Prudential Classification of Virtual Assets

5.1. Virtual assets shall be classified in three groups, namely:

i. ***Group 1a Virtual Assets:*** tokenised traditional assets that confer the same level of legal rights as ownership of the traditional (non-tokenised) version of the asset and that meet the classification conditions set out in the ***Annex***;

ii. ***Group 1b Virtual Assets:*** virtual assets with an effective stabilisation mechanism and that meet the classification conditions set out in the ***Annex***. These virtual assets may not confer the same level of legal rights as ownership of a traditional asset and seek to link the value of a virtual asset to the value of a traditional asset or a pool of traditional assets through a stabilisation mechanism. Virtual assets under this category must be redeemable for underlying traditional asset(s) (e.g.

cash, bonds, commodities, equities). They must satisfy the requirements for effective stabilisation mechanism and redemption risk tests as set out in the ***Annex***; and

iii. Group 2 Virtual Assets: virtual assets that do not qualify as Group 1a or Group 1b Virtual Assets.

5.2. Classification of virtual assets as Group 1a and Group 1b Virtual Assets shall be subject to the approval of the Bank.

5.3. Banks shall ensure that the classification conditions are met on an ongoing basis.

6. Prudential Treatment of Virtual Assets

Minimum Capital Requirements for Credit Risk for Group 1 Virtual Assets

6.1. The risk weighted assets for Group 1a Virtual Assets (tokenised traditional assets) in the banking book shall be determined as set out in the *Guideline on Standardised Approach to Credit Risk* for the relevant non-tokenised traditional assets.

6.2. Group 1a Virtual Assets which are tokenised versions of the instruments included on the list of eligible financial collateral set out in the *Guideline on Standardised Approach to Credit Risk* may qualify for recognition as eligible collateral subject to the following conditions:

i. the tokenised traditional asset meets the eligibility requirements for collateral requirements set out in the *Guideline on Standardised Approach to Credit Risk*; and

ii. there is no material increase in the volatility in values and holding periods of the tokenised traditional asset under distressed market conditions compared with the traditional asset or pool of traditional assets.

6.3. The minimum capital requirements for credit risk for Group 1b Virtual Assets in the banking book shall be determined by the Bank on a case-by-case basis and shall be at least equal to the value of exposure amount.

Minimum Capital Requirements for Market Risk for Group 1 Virtual Assets

6.4. Banks shall map the Group 1 Virtual Assets into the relevant risk category and comply with the market risk capital requirements and reporting requirements as set out in the *Guideline on Measurement and Management of Market Risk*.

6.5. Banks shall ensure that:

i. all instruments, including derivatives and off-balance sheets positions, which are affected by changes in Group 1 Virtual Assets prices, are included;

ii. each Group 1 Virtual Assets position are expressed in terms of their quantity and converted at the current spot price into the bank's reporting currency;

iii. the Group 1 Virtual Assets are subject to the same risk classes as the one used for traditional assets they digitally represent (i.e. interest rate risk, equity risk, FX risk and commodities risk); and

iv. options involving Group 1 Virtual Assets are subject to the same treatment for options as the one defined for traditional assets they digitally represent.

Minimum Capital Requirements for Credit and Market Risk for Group 2 Virtual Assets

6.6. The minimum capital requirements for credit risk and market risk for Group 2 Virtual Assets shall be determined by the Bank on a case-by-case basis. The minimum capital requirement for credit risk and market risk shall be at least equal to the value of exposure amount.

Minimum Capital Requirements for Operational Risk: Infrastructure Risk for Virtual Assets

6.7. Banks shall apply an add-on the capital requirement for all exposures to virtual assets. The add-on to capital requirements will initially be set as follows:

i. for exposures in the banking book, the risk weight that will apply to the exposures shall be increased by 2.5 percentage points; and

ii. for exposures in the trading book, total market risk weighed assets must be increased by an amount equal to 2.5% of the exposure value.

6.8. The add-on for infrastructure risk described above does not apply to virtual assets that are issued/backed by central banks.

6.9. The Bank may prescribe higher add-on factors for Group 2 Virtual Assets on a case-to-case basis.

Additional Capital Requirements

6.10. Banks shall take into consideration any potential impact of virtual assets on their business in their internal capital adequacy assessment.

6.11. Banks shall ensure that their stress testing frameworks incorporate the risks associated with the virtual asset related activities.

6.12. Banks shall maintain additional capital for risks not sufficiently captured under the minimum regulatory capital requirements for operational risk, credit risk, market risk and other identified risks.

Minimum Liquidity Risk Requirements

6.13. Banks shall identify the liquidity risks associated with virtual assets and apply the principles and standards prescribed in the *Guideline on Liquidity Risk Management*.

6.14. Banks shall assess additional risks that may be present with virtual assets in comparison to their equivalent traditional assets, and consider the relative lack of historical data when determining the liquidity risk requirements for virtual assets.

6.15. Cash inflows and outflows including assets, liabilities and contingent exposures, should be subject to the same treatment as for their equivalent traditional assets.

6.16. Group 1 Virtual Assets that are tokenised versions of High-Quality Liquid Assets (HQLA) may be considered as HQLA provided that the equivalent traditional asset and their tokenised version both satisfy the characteristics and eligibility criteria of HQLA set out in the *Guideline on Liquidity Risk Management.*

6.17. The run off rates to be applied on inflows and outflows associated with Group 1b and Group 2 Virtual Assets shall be determined, on a case-to-case basis, by the Bank.

Exposure Limits

6.18. Banks shall set internal concentration risk limits for their virtual asset related activities. This shall, inter alia, include risk limits for each type of virtual asset and risk limits by issuers/ redeemers of virtual assets as well as other relevant counterparties.

6.19. The counterparty credit risk exposures arising from virtual assets related activities shall be subject to the regulatory credit concentration limits set out in the *Guideline on Credit Concentration Risk.*

6.20. The aggregate direct and indirect exposure of a bank to Group 2 Virtual Assets shall not exceed 1 per cent of its Tier 1 Capital. The limit shall apply on the gross exposure and there shall be no netting or recognition of diversification benefits.

7. Risk, Compliance and Assurance Function

7.1. The risk function shall ensure that the risk management framework adequately captures the risks associated with virtual asset related activities and that relevant reports are regularly submitted to the board and the senior management. The risk function shall conduct independent risk monitoring regarding compliance with set strategy, policies, risk appetite and risk limits.

7.2. The compliance function shall conduct periodic reviews to ensure adherence to applicable laws and regulations in respect of virtual asset related activities.

7.3. The internal audit shall perform regular reviews of the adequacy, appropriateness and effectiveness of the risk management and internal control framework for managing risks associated with virtual asset related activities.

8. Reporting Requirements

8.1. Banks shall submit a quarterly report on virtual asset related activities to the Bank in such form and manner prescribed by the Bank.

9. Disclosure Requirements

9.1. Banks shall disclose, at least on an annual basis, in their annual reports, their material virtual asset related activities, including their direct and indirect exposure amounts for each of these activities.

Bank of Mauritius
Xx Month 2022

Annex – Classification Conditions for Group 1 Virtual Assets

(As set out in the BCBS Consultative Document- Second Consultation on the prudential treatment of cryptoasset exposures)

Group 1 Virtual Assets consist of:

a. Group 1a Virtual Assets – Tokenised traditional assets that meet the classification conditions; and

b. Group 1b Virtual Assets – Virtual assets with effective stabilisation mechanism that meet the classification conditions.

Classification condition 1:

The virtual asset either is a tokenised traditional asset or has a stabilisation mechanism that is effective at all times in linking its value to an underlying traditional asset or a pool of traditional assets.

Tokenised traditional assets

1.1 Tokenised traditional assets will only meet classification condition 1 if they satisfy all the following requirements:

i. They are digital representations of traditional assets using cryptography, DLT or similar technology to record ownership;

ii. They pose the same level of credit and market risk as the traditional (non-tokenised) form of the asset. In practice, this means the following for tokenised traditional assets:

a. *Bonds, loans, claims on banks (including in the form of deposits), equities and derivatives.* The virtual asset must confer the same level of legal rights as ownership of these traditional forms of financing (eg rights to cash flows, claims in insolvency etc). In addition, there must be no feature of the virtual asset that could prevent obligations to the bank being paid in full when due as compared with a traditional (non-tokenised) version of the asset.

b. *Commodities.* The virtual asset must confer the same level of legal rights as traditional account-based records of ownership of a physical commodity.

c. *Cash held in custody.* The virtual assets must confer the same level of legal rights as cash held in custody.

1.2 Virtual assets do not meet the condition set out in section 1.1 above if they:

i. first need to be redeemed or converted into traditional assets before they receive the same legal rights as direct ownership of traditional assets; or

ii. through their specific construction, they involve additional counterparty credit risks relative to traditional assets.

Virtual assets with effective stabilisation mechanism

1.3 Virtual assets that have a stabilisation mechanism will only meet classification condition 1 if they satisfy all of the following requirements:

i. The virtual asset is designed to be redeemable for a predefined amount of a reference asset or assets (eg 1 USD, 1 Oz gold) or cash equal to the current market value of the reference asset(s) (eg USD value of 1 Oz gold). The value of the reference asset(s) to which one unit of the virtual asset is designed to be redeemable is referred to as the "peg value".

ii. The stabilisation mechanism is designed to minimise fluctuations in the market value of the virtual assets relative to the peg value. In order to satisfy the "effective at all times" condition, banks must have a monitoring framework in place verifying that the stabilisation mechanism is functioning as intended. To this end, banks confirm that the virtual asset meets the redemption risk test and the basis risk test outlined under sections 1.4.1 and 1.4.2 below.

iii. The stabilisation mechanism enables risk management similar to the risk management of traditional assets, based on sufficient data or experience. For newly established virtual assets, there may be insufficient data and/or practical experience to perform a detailed assessment of the stabilisation mechanism. Evidence must be provided to satisfy supervisors of the effectiveness of the stabilisation mechanism, including the composition, valuation and frequency of valuation of the reserve asset(s) and the quality of available data.

iv. There exists sufficient information that banks use to verify the ownership rights of the reserve assets upon which the stable value of the virtual asset is dependent. In the case of underlying physical assets, banks must verify that these assets are stored and managed appropriately. This monitoring framework must function regardless of the virtual asset issuer. Banks may use the assessments of independent third parties for the purposes of verification of ownership rights only if they are satisfied that the assessments are reliable.

1.4 Virtual assets that have a stabilisation mechanism will only meet classification condition 1 if they pass the following two tests:

1.4.1 <u>*Redemption risk test*</u>

The objective of this test is to ensure that the reserve assets are sufficient to enable the virtual assets to be redeemable at all times, including during periods of extreme stress, for the peg value. To pass the redemption risk test, the bank must ensure that the virtual asset arrangement meets the following conditions:

i. *Value and composition of reserve assets*. The value of the reserve assets (net all non-virtual asset claims on these assets) must at all times, including during periods of extreme stress, equal or exceed the aggregate peg value of all outstanding virtual assets. If the reserve assets expose the holder to risk in addition to the risks arising from the reference assets, the value of the reserve

assets must sufficiently overcollateralise the redemption rights of all outstanding virtual assets. The level of overcollateralisation must be sufficient to ensure that even after stressed losses are incurred on the reserve assets, their value exceeds the aggregate value of the peg of all outstanding virtual assets.

ii. *Management of reserve assets*. The governance arrangements relating to the management of reserve assets must be comprehensive and transparent. They must ensure that:

a. The reserve assets are managed and invested with an explicit legally enforceable objective of ensuring that all virtual assets can be redeemed promptly at the peg value, including under periods of extreme stress.

b. A robust operational risk and resilience framework exists to ensure the availability and safe custody of the reserve assets.

c. A mandate that describes the types of assets that may be included in the reserve must be publicly disclosed and kept up to date.

d. The composition and value of the reserve assets are publicly disclosed on a regular basis. The value must be disclosed at least daily and the composition must be disclosed at least weekly.

e. The reserve assets are subject to an independent external audit at least annually to confirm they match the disclosed reserves and are consistent with the mandate.

1.4.2 *Basis risk test*

The objective of the basis risk test is to ensure that the holder of a virtual asset can sell it in the market for an amount that closely tracks the peg value. To pass the basis risk test, banks must first monitor daily the percentage difference between the peg value of the virtual asset and its market value (using a consistent source for the market value from prices quoted on a regulated market/exchange). Banks must calculate the "peg-to-market value difference" as:

[(peg value – market value) / peg value], expressed in basis points.

Banks must then use the following thresholds to determine whether the basis risk test is fully passed, narrowly passed or failed:

i. If the peg-to-market value difference does not exceed 10bp more than 3 times over the prior 12 months, the virtual asset has "fully passed" the basis risk test;

ii. If the peg-to-market value difference exceeds 20bp more than 10 times over the prior 12 months, the virtual asset has "failed" the basis risk test; and

iii. If the virtual asset has neither "fully passed" nor "failed" the basis risk test, it is considered to have "narrowly passed" the basis risk test. Virtual assets that meet all of the classification conditions for inclusion in Group 1b, but only narrowly

pass the basis risk test will be considered to have met all the classification conditions and will not be classified in Group 2. However, such virtual assets will be subject to a risk-weighted asset (RWA) adjustment as described in section 1.5 below.

1.5 Banks that have exposures to virtual assets that only narrowly pass the basis risk test must apply a capital add-on as follows:

i. for exposures in the banking book, total credit RWA must be increased by an amount equal to 100% of the exposure value; and

ii. for exposures in the trading book, total market RWA must be increased by an amount equal to 100% of the exposure value.

1.6 For a stablecoin to be classified as Group 1b, the issuer must be supervised and regulated by a supervisor that applies prudential capital and liquidity requirements.

1.7 The following types of stabilisation mechanisms do not meet classification condition 1:

i. stabilisation mechanisms that reference other virtual assets as underlying assets (including those that reference other virtual assets that have traditional assets as underlying); or

ii. stabilisation mechanisms that use protocols to increase or decrease the supply of the virtual assets;

<u>Classification condition 2</u>
All rights, obligations and interests arising from the virtual asset arrangement are clearly defined and legally enforceable in all the jurisdictions where the asset is issued and redeemed. In addition, the applicable legal framework(s) ensure(s) settlement finality.

2.1. Banks shall conduct a legal review of the virtual asset arrangement to ensure this condition is met, and make the review available to the Bank upon request.

Tokenised traditional assets

2.2. Tokenised traditional assets will only meet classification condition 2 if they satisfy the following requirements at all times:

i. the virtual asset arrangements must ensure full transferability, settlement finality and full redeemability; and

ii. banks must ensure that the virtual asset arrangements are properly documented.

Virtual assets with effective stabilisation mechanism

2.3. Virtual assets that have a stabilisation mechanism will only meet classification condition 2 if they satisfy the following requirements at all times:

i. the virtual asset arrangements must ensure full transferability and settlement finality. Virtual assets with stabilisation mechanisms must ensure full redeemability (i.e. the ability to exchange virtual assets for amounts of pre-defined assets such as cash, bonds, commodities, equities or other traditional assets) at all times and at their peg value. In order for a virtual asset arrangement to be considered as having full redeemability, it must allow for the redemption to be completed within 5 calendar days of the redemption request at all times.

ii. the virtual asset arrangements are properly documented and clearly define which parties have the right to redeem; the obligation of the redeemer to fulfil the arrangement; the timeframe for this redemption to take place; the traditional assets in the exchange; and how the redemption value is determined. These arrangements must also be valid in instances where parties involved in these arrangements may not be located in the same jurisdiction where the virtual asset is issued and redeemed. At all times, settlement finality in virtual asset arrangements must be properly documented such that it is clear when key financial risks are transferred from one party to another, including the point at which transactions are irrevocable. Banks must ensure that the documentation described in this paragraph is publicly disclosed by the virtual asset issuer. If the offering of the virtual asset to the public has been approved by the relevant regulator on the basis of this public disclosure, the condition in section 2.3(ii) will be considered fulfilled. Otherwise, an independent legal opinion would be needed to confirm section 2.3(ii) has been met.

Classification condition 3

The functions of the virtual asset and the network on which it operates, including the distributed ledger or similar technology on which it is based, are designed and operated to sufficiently mitigate and manage any material risks.

3.1. To meet classification condition 3 the following requirements must be met:

i. The "sufficient" condition would be satisfied if the functions of the virtual asset, such as issuance, validation, redemption and transfer of the virtual assets, and the network on which it runs do not pose any material risks that could impair the transferability, settlement finality or redeemability of the virtual asset. To this end, entities performing activities associated with these functions must follow robust risk governance and risk control policies and practices to address risks including, but not limited to: credit, market and liquidity risks; operational risk (including outsourcing, fraud and cyber risk) and risk of loss of data; and various non-financial risks, such as data integrity; operational resilience (ie operational reliability and capacity); third party risk management; and Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT).

ii. Networks that fulfil this condition would be those where the key aspects are well-defined such that all transactions and participants are traceable. Key aspects include:

a. the operational structure (ie whether there is one or multiple entities that perform core function(s) of the network);

b. degree of access (ie whether the network is restricted or un-restricted);

c. technical roles of the nodes (ie whether there is a differential role and responsibility among nodes); and

d. the validation and consensus mechanism of the network (ie whether validation of a transaction is conducted with single or multiple entities).

Examples of these entities include but are not limited to: issuers, operators of the transfer and settlement systems for the cryptoasset; administrators of the cryptoasset stabilisation mechanism and custodians of any underlying assets supporting the stabilisation mechanism.

Classification condition 4

Entities that execute redemptions, transfers, storage or settlement finality of the virtual asset, or manage or invest reserve assets, are regulated and supervised, or subject to appropriate risk management standards.

4.1. Entities subject to condition 4 include operators of the transfer and settlement systems for the virtual asset, wallet providers, administrators of the virtual asset stabilisation mechanism and custodians of any underlying assets supporting the stabilisation mechanism. Node validators may be subject to appropriate risk management standards as an alternative to being regulated and supervised.