BANK OF MAURITIUS

Guideline for Virtual Asset related Activities

November 2024

Page intentionally left blank

TABLE OF CONTENTS

Page intentionally left blank

INTRODUCTION

Background

Virtual assets related activities expose banks to a number of risks including liquidity risk, credit risk, market risk, operational risk (including fraud risk and cyber risks), money laundering and terrorist financing and proliferation risks, legal risks and reputational risks.

Purpose

This guideline sets out the principles to be followed by banks involved in activities related to virtual assets. The guideline is based on standards of the Basel Committee on Banking Supervision on cryptoassets 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 banks licensed under the Banking Act 2004 involved in virtual asset related activities, as defined under this guideline.

Effective date

The Guideline shall be applicable with immediate effect.

Transitional provisions

Banks shall ensure full compliance with this Guideline by 31 May 2025.

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" refers to:

i. the board of directors of a bank;

ii. the local advisory board/committee of a branch of a foreign bank; or

iii. where a branch of a foreign bank has no local advisory board, the responsibilities assigned to the board shall rest on the Chief Executive Officer of the branch;

"Distributed Ledger Technology" has the same meaning as in the VAITOS Act;

"exposure" includes on- or off-balance sheet amounts that give rise to credit, market, operational and/or liquidity risks;

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

"initial token offerings" or "ITO" has the same meaning as in the VAITOS Act;

"issuer of initial token offerings" has the same meaning as in the VAITOS Act;

"nodes" refer to participants (entities including individuals) in distributed ledger networks that record and share data across multiple data stores (or ledgers);

"operators" refer to a single administrative authority in charge of managing a virtual asset arrangement, performing functions that may include issuing (putting into circulation) a centralised virtual asset, establishing the rules for its use; maintaining a central payment ledger; and redeeming (withdraw from circulation) the virtual asset;

"peg value" refers to the value of the reference asset(s) to which one unit of the virtual asset is designed to be redeemable;

"public ('permissionless') ledger" refer to ledgers where the validation of transactions can be done by any participating agent, or distributed among several agents or intermediaries, which could be unknown to the users;

"private ('permissioned') ledger" refer to ledgers which restrict and pre-define the scope of validators, with the validating entities known to the users;

"redeemers" refer to entities responsible for exchanging the virtual asset for the traditional asset. It does not necessarily need to be the same as the entity responsible for organising the issuance of the virtual asset;

"stablecoins" are virtual assets that aim to maintain a stable value relative to a specified asset, or a pool or basket of assets;

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

"validators" refer to an entity that commits transactions blocks to the distributed ledger network;

"virtual asset", for the purpose of this guideline: means a digital representation of value that may be digitally traded or transferred, and may be used for payment or investment purposes and includes private digital assets, that depend on cryptography and distributed ledger or similar technologies and tokenised traditional assets as well as dematerialized securities (securities that have been moved from physical certificates to electronic book-keeping) that are issued through DLT or similar technologies; but –
(a) does not include a digital representation of fiat currencies; and
(b) does not include dematerialised securities that use electronic versions of traditional registers

and databases which are centrally administered.

"virtual asset exchange" has the same meaning as in the VAITOS Act;

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

i. activities or operations of virtual asset service providers and issuers 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 asset service providers;

    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 service providers, issuers of initial token offerings and significant dealings in virtual assets;

    e. collaterals comprising of virtual assets and/or linked to virtual assets; and

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

"virtual asset service provider" has the same meaning as in the VAITOS Act;

"virtual asset wallet services" has the same meaning as in the VAITOS Act; and

"virtual token" has the same meaning as in the VAITOS Act.

1. Responsibilities of Board

1.1. The board shall:

i. ensure that a comprehensive risk assessment is conducted before a bank engages into virtual asset related activities and that relevant controls and mitigants are implemented to address the identified risks. The risk assessment should be duly documented and approved by the board;

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

iii. approve and periodically (at least annually) review the strategy, risk appetite, risk limits, risk management framework and relevant policies for virtual asset related activities;

iv. ensure that virtual assets are duly classified at the outset and that the classification criteria are met on an ongoing basis;

v. 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 virtual asset related activities;

vi. 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;

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

viii. ensure that it receives periodic risk reports on virtual asset related activities and is promptly notified of any material development.

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 with virtual asset related activities;

iii. ensure that virtual assets related activities are subject to a comprehensive risk assessment, and implement relevant controls/ mitigants to address the identified risks;

iv. ensure that virtual assets meet the classification criteria on an ongoing basis and that requisite approvals are in place for the classification;

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

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

vii. ensure compliance with applicable legal and regulatory requirements;

viii. regularly review the effectiveness of the framework, policies, tools and controls in place; and

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

3. Regulatory Approval and Notification

3.1. Banks shall ensure compliance with the requirements of section 30 of the Act in respect of investments and other activities involving tokenised shares, stocks and other assets.

3.2. 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; and

ii. applying, through their 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.

3.3. The application for approval shall be accompanied by the risk assessment report of the bank as approved by the board covering the classification of the virtual assets, the identified risks, the potential impact and the risk mitigating measures.

3.4. The Bank shall be notified whenever banks propose to take any exposure in virtual assets which do not qualify as Group 1a and 1b Virtual assets. The notification shall include the risk assessment as approved by the board covering the classification of the virtual assets, the identified risks, the potential impact and the risk mitigating measures, the approval received from the board, the risk limits and the proposed treatment with respect to measurement of the risk and the computation of the risk weighted assets and capital/liquidity requirements, including the run-off rates for the computation of the

Liquidity Coverage Ratio. The notification shall be done at least 60 days before the bank proposes to take the exposure.

3.5. The Bank may override the classification and impose higher capital requirement based on the characteristics of the underlying assets.

3.6. The approval of the Bank is not required for the provision of banking services to virtual asset service providers, issuers of initial token offering and customers dealing in virtual asset related activities. This includes the processing of payment transactions in respect of purchase, sale and redemption of virtual assets in exchange of fiat currencies.

4. Risk Management Framework

4.1. Banks shall establish policies and procedures to identify, assess and mitigate the risks including but not limited to credit risk, liquidity risk, concentration risk, market risk, operational risk (including fraud, technology and cyber risks), money laundering and terrorism financing and proliferation risks, legal and reputational 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. Banks shall ensure that the virtual asset related activities comply with the risk appetite and other risk limits approved by the board.

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

i. ensure that the board, on a collective basis, and the relevant members of the senior management have the requisite expertise and skills for an effective oversight over the activities and evaluation of the associated risks;

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

iii. undertake a comprehensive risk assessment to ensure that the associated risks that may arise are duly identified, assessed, understood and mitigated;

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

v. 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;

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

vii. satisfy themselves that the virtual asset related activities, including the virtual assets service providers are duly licensed and regulated.

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

Credit Risk

4.6. 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 asset related activities and collaterals comprising of virtual assets.

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

4.8. 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.

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

Concentration Risks

4.10. 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.

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

4.12. 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.

Liquidity Risk

4.13. Banks shall assess the potential impact of their investments/ other activities related to virtual assets on their liquidity position and factor same 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.

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

4.15. 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.

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

4.17. 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 Bank's *Guideline on Liquidity Risk Management.*

4.18. 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.

Market Risk

4.19. 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.

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

Operational Risk and Cyber and Technology Risk

4.21. Banks shall ensure that their internal operational risk and cyber and technology risk management frameworks duly cover the risks associated with virtual asset related activities, 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 (reliability of the source code, governance around protocols and integrity of the technology, capacity constraints, track record of the underlying technology, etc.), validating design of the Distributed Ledger Technology (permissionless or permissioned ledger), service accessibility (inability to access/recover virtual assets due to loss of keys; unauthorized access/ loss of access to the cryptographic keys due to cyber-attacks) , trustworthiness of the node operators (whether the nodes run by public/private institutions/ individuals);and operator diversity (whether the nodes are run by a single or are distributed among many operators);

ii. cyber and technology/ fraud 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; inadequate disclosure to customers (data privacy and data retention, etc.), uncertain legal status.

Valuation Risk

4.22. Banks shall ensure that there are relevant operational processes for the valuation of the virtual assets.

Money Laundering and Terrorism Financing and Proliferation Risk

Customer Risk

4.23. Banks shall put in place appropriate policies and procedures to support the adequate conduct of customer due diligence (identification, verification and securing of information on the ultimate beneficial owner), prior to opening an account or establishing a business relationship with virtual asset service providers, issuers of initial token offering or customers dealing in virtual assets. The bank should gather sufficient information on the customer during the identification and verification stage to enable it to understand the customer's nature of business and build a risk profile. The risk profile of the customer will determine the level and type of ongoing monitoring required and support the bank's decision whether to enter into, continue, or terminate the business relationship.

4.24. The risk profiles can apply at the customer level (e.g., nature and volume of trading activity, origin of virtual funds deposited etc.) or at the cluster level, where a cluster of customers displays homogenous characteristics (e.g., customers conducting similar types of transactions or involving the same virtual assets). The level of risk associated with the customer or the cluster of customers involved in dealings with virtual assets will in turn determine the level of due diligence that the bank will be applying to the individual customer and his transactions and the level of reviews that would be conducted.

4.25. Banks shall apply a 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, issuers of initial token offering, customers involved in virtual asset related activities, or when engaging in virtual asset related activities themselves or through their subsidiaries.

4.26. 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 activities of the virtual asset service providers, virtual asset related activities and customers involved with such activities. Banks shall take appropriate measures to manage and mitigate those risks. Those measures should include proper risk assessment taking into consideration all the relevant risk factors before determining the level of the overall risk, and the appropriate type and extent of mitigation applied, keeping the risk assessment up to date with conduct of timely reviews based on the risk category and documenting the risk assessment.

4.27. As part of the risk mitigating process, banks shall develop and implement policies procedures and controls to effectively manage and mitigate the ML/TF/PF risks that have been identified with the VASPs, virtual assets related activities and customers involved with such activities. The implementation of those policies procedures and

controls should be monitored and banks shall regularly update, and where necessary enhance their internal policies, controls and procedures.

4.28. When a bank is not capable of applying the appropriate level of due diligence or their risk mitigation measures are not adequate to the level of ML/TF/PF risk being exposed, they shall abstain from entering into the business relationship or terminate the already-existing business relationship as the case may be and consider the filing of an STR to the Financial Intelligence Unit as stipulated under Section 14 of the FIAMLA and in accordance with the FIAML Regulations 2018.

4.29. Banks shall continuously identify and assess ML/TF/PF risks that may arise in relation with new products which fall within the definition of virtual asset related activities which are developed by the VASPs and offered to customers. Banks shall also ensure that the virtual asset service providers have undertaken a risk assessment prior to the launch of the new products or the technology or delivery channel / mechanism being used for the product.

4.30. Banks shall always apply the risk threshold allocated to this type of business in the National Risk Assessment exercise conducted at the National level notwithstanding that their assessment of the risk pertaining to virtual asset may be lower.

Transaction Monitoring

4.31. Banks shall have adequate systems in place to conduct transaction monitoring of activities held in the accounts of virtual asset service providers, or customers involved with virtual asset related activities following a risk-based approach. The extent of monitoring, i.e., frequency and intensity of monitoring should commensurate with the risk profile of the customer. Banks shall, however, ensure that the risk weight allocated to virtual asset service providers or customers involved with virtual asset related activities should not be below the risk threshold allocated to this type of business in the National Risk Assessment exercise conducted at the National level, notwithstanding that the bank's assessment of the risk pertaining to virtual asset may be lower.

4.32. In establishing the scenarios and calibrating the transaction monitoring system, banks shall consider the customer's risk profile, information collected during the conduct of customer due diligence, information obtained from law enforcement bodies and other authorities in its jurisdiction and the approach to risk allocation in the National Risk Assessment.

4.33. The FATF has, in its report entitled the Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing[1], available at Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (fatf-gafi.org), laid down a number of red flag indicators that could suggest that virtual assets are used for criminal activity. These red flags are summarised under ***Annex 2***.

[1] The report is available at available at Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (fatf-gafi.org).

Sanctions screening

4.34. Sanctions obligations apply to crypto / virtual asset service providers / exchanges, custodian and wallet providers as they do to other financial institutions. Financial institutions should be aware that some sanction lists may now include information on wallet numbers in addition to / instead of names. Sanctions screening remains a critical component in the exercise of due diligence. Banks should implement robust screening mechanism that leverage on advanced technological solutions to detect and prevent transactions involving sanctioned individuals, entities or jurisdictions, as well as virtual asset service providers/ exchanges and digital wallets identification numbers in real time.

4.35. 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 and are strictly prohibited to engage in or support anonymous virtual asset 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 1***;

ii. ***Group 1b Virtual Assets:*** virtual assets with an effective stabilisation mechanism and that meet the classification conditions set out in the ***Annex 1***. 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 1***; and

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

5.2. Banks shall ensure that the classification conditions are met on an ongoing basis. They must fully document the information used in determining compliance with the classification conditions at the outset and on an ongoing basis and make this available to the Bank on request. The Bank may override the classification depending on the characteristics of the virtual assets.

5.3. With respect to Group 1b virtual assets, banks must

i. ensure that they have an adequate understanding, at acquisition and thereafter on a regular basis, of the stabilisation mechanism of the virtual asset and of its effectiveness; and

ii. conduct statistical or other tests demonstrating that the virtual asset maintains a stable relationship in comparison to its reference asset (basis risk test).

6. Accounting Classification for Virtual Assets

6.1 Investments in virtual assets will not be subject to the deduction requirement that applies to intangible assets set out in paragraph 24 of the Guideline on Scope of Application of Basel III and Eligible Capital, even in cases where they are classified as an intangible under the applicable accounting standard.

7. Capital Requirements for Virtual Assets

Minimum Capital Requirements for Credit Risk for Group 1 Virtual Assets

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

7.2 Group 1a Virtual Assets which are tokenised versions of the instruments included on the list of eligible financial collateral set out in the Bank's *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 Bank's *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.

7.3 Banks that have banking book exposures to Group 1b virtual assets must analyse their specific structures and identify all risks that could result in a loss and include the relevant credit Risk Weighted Assets. This shall include credit risk weighted assets associated with the issuer of the reference assets, credit risk weighted assets associated with the redeemer of the virtual assets and credit risks weighted assets to reflect contractual obligations of banks to redeem the virtual assets, as applicable.

7.4 Group 1b virtual assets are not eligible forms of collateral for the purposes of recognition as credit risk mitigation since the process of redemption may add counterparty risk that is not present in a direct exposure to a traditional asset.

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

Minimum Capital Requirements for Market Risk for Group 1 Virtual Assets

7.6 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 Bank's *Guideline on Measurement and Management of Market Risk*.

7.7 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.

7.8 The minimum capital requirements for market risk for Group 1b Virtual Assets shall be determined by the Bank on a case-to-case basis. The minimum capital requirement for market risk shall be at least equal to the value of exposure amount.

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

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

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

7.10 Banks shall apply an add-on to the capital requirement for all exposures to virtual assets. The add-on to capital requirements shall 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.

7.11 The add-on for infrastructure risk described above does not apply to Central Bank Digital Currencies or other virtual assets that are issued/backed by central banks.

Additional Capital Requirements

7.12 Banks shall take into consideration any potential impact of virtual assets on their business in their Internal Capital Adequacy Assessment.

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

7.14 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.

8. Risk, Compliance and Assurance Function

8.1 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.

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

8.3 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.

9. Reporting Requirements

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

10. Disclosure Requirements

10.1 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 and the governance and risk management framework.

Bank of Mauritius
13 November 2024

Annex 1 – Classification Conditions for Group 1 Virtual Assets[2]

Group 1 Virtual Assets consist of:

a. Group 1a Virtual Assets – Tokenised traditional assets that meet the classification conditions 1-4; and

b. Group 1b Virtual Assets – Virtual assets with effective stabilisation mechanism **linking its value to an underlying traditional asset or a pool of traditional assets** and that meet the classification conditions 1-4.

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 shall only meet classification condition 1 if they satisfy all the following requirements:

i. They are digital representations of traditional assets using cryptography, Distributed Ledger Technologies 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 (e.g., 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:

[2] The text below is based from the Basel Framework for 'cryptoassets exposures' (SCO60).

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.

Classification conditions for Group 1b Virtual Assets – Virtual assets with effective stabilisation mechanism

1.3 The cryptoasset is designed to be redeemable for a predefined amount of a reference asset or assets (e.g., 1 USD, 1 oz gold) or cash equal to the current market value of the reference asset(s) (e.g., USD value of 1 oz gold).

1.4 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.

1.5 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. Banks must document and make available to supervisors on request the assessment they conducted and the evidence used to determine 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.

1.6 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.

1.7 The virtual asset passes the redemption test set out in paragraph 1.8 below and the issuer is supervised and regulated by a supervisor that applies prudential capital and liquidity requirements to the issuer.

1.8 *Redemption risk test*

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:

1.8.1 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.

1.8.2 Asset quality criteria for reserve assets for virtual assets pegged to currencies

For virtual assets that are pegged to one or more currencies, the following requirements must be met:

(a) The reserve assets must be comprised of assets with minimal market and credit risk where:

(i) the reserve assets should consist mainly of assets with short-term maturities and high credit quality[3]; and

(ii) the reserve assets have a proven record of relative stability of market terms (e.g., low volatility of traded prices and spreads) even during stressed market conditions.

(b) The reserve assets must be capable of being liquidated rapidly with minimal adverse price effect where:

(i) each reserve asset has a proven record as a reliable source of liquidity in the markets even during stressed market conditions, and those that are marketable securities are traded in large, deep and active markets;

(ii) if the price of a reserve asset is determined by a pricing formula, the formula must be easy to calculate and not depend on strong assumptions, and the inputs into the pricing formula must be publicly available;

(iii) the reserve assets provide sufficient daily liquidity to meet "instant" redemption requests from the virtual asset holders; and

(iv) the reserve assets are placed in structures that are bankruptcy remote from any party that issues, manages or is involved in the stablecoin operation or custodies the reserve assets[4].

(c) Eligible types of reserve assets include, but are not limited to:

(i) central bank reserves, to the extent that the stablecoin issuer is eligible to hold these reserves and the central bank's policies allow these reserves to be drawn down in times of stress;

[3] These include: (i) marketable securities representing claims on or guaranteed by sovereigns or central banks with a low risk of default (eg subject to a 0% risk weight under the standardised approach to credit risk or equivalent, or subject to a non-0% risk weight to the extent that the virtual asset is pegged to the domestic currency of the sovereign or central bank); and (ii) deposits at highly rated banks with a low risk of default.

[4] In the case of cash deposits in a bank that only provides custody services to the stablecoin, such cash deposits are not required to be bankruptcy remote from that bank, subject to it being a prudentially regulated bank that meets the conditions set out in 1.8.2(c)(iii).

(ii) marketable securities representing claims on or guaranteed by sovereigns and central banks with high credit quality[5] and cash receivable from very short-term reverse repurchase agreements on the basis that they are overcollateralised by these marketable securities[6]; and

(iii) deposits at banks with high credit quality and safeguards, such as a concentration limit applied at group level that includes entities with close links; bankruptcy remoteness of the deposits from any party that issues, manages or is involved in the stablecoin operation; and application of the Basel Framework (including the liquidity coverage ratio).

(d) The reserve assets must be denominated in the same currency or currencies in the same ratios as the currencies used for the peg value. A de minimis portion of the reserve assets may be held in a currency other than the currencies used for the peg value, provided that the holding of such currency is necessary for the operation of the virtual asset arrangement and all currency mismatch risk between the reserve assets and peg value has been appropriately hedged[7].

1.8.3 Asset quality criteria for reserve assets for virtual assets not pegged to currencies. For virtual assets that are not pegged to currencies, the reserve assets must largely include asset(s) presenting the same risk profile of the reference assets. That means, the reserve assets should include only the reference assets, except for a de minimis portion of the reserve assets that may be held in cash or bank deposit, provided that the holding is necessary for the operation of the virtual asset arrangement.

1.8.4 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.

[5] For example, securities referred to HQLA1 under paragraph 25(c) of the Guideline on Liquidity Risk Management can be considered, as well as securities representing claims on or guaranteed by a sovereign or central bank with a non-0% risk weight under the standardised approach to credit risk, to the extent that the virtual asset is pegged to the domestic currency of that sovereign or central bank.

[6] The following are excluded from the calculation of eligible reserve assets: (i) cash received from repurchase agreements and similar securities financing transactions (SFTs), which expand the balance sheet and, thus, increase leverage at the stablecoin issuer; and (ii) securities received from collateral swaps, which can allow lower quality or less liquid securities to be temporarily swapped for higher quality or more liquid securities.

[7] In case of hedging, the collateral used in credit support annex agreements should be encumbered and subtracted from what is considered the reserve asset funds.

d. An appropriate risk management framework exists to assess and monitor the risks of reserve assets, including but not limited to market risk, credit risk, concentration risk and liquidity risk. Examples include ongoing monitoring of deposit counterparties and custodians, daily valuation of reserve assets and stress testing.

e. The composition and value of the reserve assets are publicly disclosed on a regular basis. The value outstanding amount of virtual assets in circulation must be disclosed at least once every trade day and the composition must be disclosed at least weekly. This disclosed information must be verified by an independent third party at least semi-annually to confirm its completeness, fairness of valuation and accuracy.

f. The composition and value of the reserve assets and the outstanding amount of virtual assets in circulation are subject to an independent external audit at least annually to confirm they match the disclosed reserves and are consistent with the mandate.

1.9 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;

Classification condition 2

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 in both primary and secondary markets. 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.

Virtual assets must meet the following requirements to satisfy the classification condition 2:

2.1 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.

2.2 The virtual asset arrangements are properly documented at all times. For virtual assets with stabilisation mechanisms, the arrangements must 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 the virtual asset has become irrevocably and unconditionally transferred, so that key financial risks are moved from one party to another. Banks must ensure that that the documentation described in this paragraph must be 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 2.2 will be considered fulfilled. Otherwise, an independent legal opinion would be needed to confirm section 2.2 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 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 (i.e. operational reliability and capacity); third party risk management; and Anti-Money Laundering/Countering the Financing of Terrorism and Proliferation (AML/CFT).

ii. All key elements of the network must be well-defined such that all transactions and participants are traceable. Key elements include:

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

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

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

   d. the validation and consensus mechanism of the network (i.e., 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 virtual asset; administrators of the virtual asset

stabilisation mechanism and custodians of any underlying assets supporting the stabilisation mechanism.

Classification condition 4

All entities that execute redemptions, transfers, storage or settlement of the virtual asset, or manage or invest reserve assets, must be regulated and supervised, or subject to appropriate risk management standards, and have in place and disclose a comprehensive governance framework.

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.

Annex 2 - Red Flag Indicators for Virtual Assets being used for Criminal Activity
(As set out in the FATF Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing)

1. Transactions

The size and frequency of transactions of virtual asset-related activities should raise suspicion of potential criminal activity. For instance:

a. Structuring virtual assets transactions (e.g., exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds;

b. Making multiple high-value transactions;

c. Transferring virtual assets immediately to multiple virtual asset service providers, especially to virtual asset service providers registered or operated in another jurisdiction;

d. Depositing virtual assets at an exchange and then often immediately withdrawing/converting it; or

e. Accepting funds suspected as stolen or fraudulent.

2. Transaction patterns

Irregular, unusual, or uncommon patterns of transactions usually indicate the misuse of virtual assets for ML/TF purposes:

a. Conducting a large initial deposit to open a new relationship with a virtual asset service provider:

   i. while the amount funded is inconsistent with the customer profile;

   ii. funding the entire deposit, the first day it is opened;

   iii. the customer starts to trade the total amount or a large portion of the amount on that same day or the day after; and

   iv. or if the customer withdraws the whole amount the day after.

b. Transaction involving the use of multiple virtual assets, or multiple accounts, multiple transactions by multiple persons, using multiple IP addresses and involves large amounts;

c. Small transactions originating from multiple wallets, but converted as a whole into fiat currency;

d. Conducting virtual asset fiat currency exchange at a potential loss; and

e. Converting a large amount of fiat currency into virtual assets, or a large amount of one type of virtual asset into other types of virtual assets.

3. Anonymity Principle

The various technological features currently used increase anonymity and add hurdles to the detection of criminal activity by Law Enforcement Agencies. These features include the use of more than one type of virtual assets for one particular transaction or the use of privacy coins, the use of decentralised/unhosted, hardware or paper wallets to transport virtual assets across borders, utilisation of the darknet to access virtual asset service provider platforms or anonymity-enhanced cryptocurrency amongst others. Banks shall have controls in place and system design to detect and prevent the occurrence of such activities through their banking platforms.

4. Senders / Recipient red flag

In relation to **senders/recipient** red flag indicators, the FATF report highlights irregularities which may be observed during the account creation such as creating separate accounts under different names, irregularities which may be observed during CDD process such as instances where the customer declines requests for KYC documents or inquiries regarding source of funds or in terms of the customer profile where a customer is known via publicly available information to law enforcement due to previous criminal association. The FATF report also warn against profile of money mules or scam victims as well as other unusual behaviours such as where a customer tries to enter into one or more virtual asset service providers from different IP addresses frequently over the course of a day.

5. Source of funds/wealth

In respect of **source of funds/wealth**, the FATF noted from the cases submitted by jurisdictions, the misuse of virtual assets often relates to criminal activities, such as illicit trafficking in narcotics and psychotropic substances, fraud, theft and extortion. In this connection, it listed some common red flags, associated with the aforementioned crimes. These include amongst others, virtual asset transactions originating from or destined to online gambling services, the use of one or multiple credit and/or debit cards that are linked to a virtual asset wallet to withdraw large amounts of fiat currency, or lack of transparency or insufficient information on the origin and owners of the funds.

6. Geographical Risks

For red flag indicators related to **geographical risks**, the FATF indicated that these risks are associated with source, destination, and transit jurisdictions of a transaction. They are also relevant to risks associated with the originator of a transaction and the beneficiary of funds that may be linked to a high-risk jurisdiction. They may also be applicable to the customer's nationality, residence, or place of business.