The Commonwealth Model Law on Stablecoins

The Commonwealth

Office of Civil and Criminal Justice Reform

The Commonwealth Model Law on Stablecoins

The Commonwealth

Commonwealth Secretariat
Marlborough House
Pall Mall
London SW1Y 5HX
United Kingdom
www.thecommonwealth.org

Views and opinions expressed in this publication are those of the authors and should in no way be attributed to the institutions to which they are affiliated or to the Commonwealth Secretariat. In addition, the authors will accept no responsibility for any actions taken or not taken on the basis of this publication.

This publication is not intended to be and should not be used as a substitute for taking legal advice in any specific situation and does not create a contractual or other legal relationship between the authors, or their affiliations, or the Commonwealth Secretariat, and anyone.

The drafting style mostly adopted in this publication is patterned from the Commonwealth Legislative Drafting Manual. There may however be instances of deviation from the style in the manual in some provisions.

Wherever possible, the Commonwealth Secretariat uses paper sourced from responsible forests or from sources that minimise a destructive impact on the environment.

Published by the Commonwealth Secretariat.

Contents

Foreword

The rapid growth of digital finance is reshaping economies across the Commonwealth and around the world. Among the most important developments is the rise of stablecoins – digital assets that are increasingly used for payments, remittances and expanding access to financial services.

For many of our member countries, particularly developing and emerging economies, this presents a real opportunity to widen financial inclusion, reduce the cost of transactions and connect more people and businesses to the global economy. But it also brings new risks – and a clear need for effective, modern regulation.

This *Model Law on Stablecoins* is designed to meet that need.

Building on the Commonwealth's *Model Law on Virtual Assets*, it provides a practical and adaptable framework to help countries regulate stablecoins in a way that supports innovation while safeguarding financial stability, protecting consumers, and strengthening trust in digital systems.

The *Model Law* offers a clear structure for licensing and oversight, robust standards for reserve management and strong safeguards against financial crime. It also reflects the realities of a fast-evolving digital landscape – remaining flexible, technology-neutral and responsive to future developments.

Importantly, this is not a one-size-fits-all solution. It is a shared resource – a framework that Commonwealth countries can adapt to their own legal systems, policy priorities and stages of development.

What makes this work particularly valuable is the breadth of expertise behind it. It has been shaped through collaboration between legal practitioners, regulators and technical experts from across the Commonwealth and beyond. Their collective experience has ensured that the *Model Law* is rigorous, practical and implementable.

It also draws on international best practice, aligning with the work of global standard-setting bodies and reinforcing the Commonwealth's commitment to secure, transparent and inclusive financial systems.

At its core, this *Model Law* reflects a wider ambition: to ensure that innovation serves people – expanding opportunity while ensuring stability and safeguarding trust.

As the global financial system evolves, the Commonwealth has a unique role to play in supporting its members to navigate change with confidence. By providing tools such as this, we aim to help countries harness the benefits of digital finance while managing its risks responsibly.

I would like to express my sincere gratitude to all those who contributed their time and expertise to this work. Their commitment reflects the very best of Commonwealth cooperation – practical, generous, and focused on shared progress.

I commend this *Model Law* to our member countries as a valuable resource in shaping the future of digital finance.

The Hon. Shirley Botchwey, Secretary-General of the Commonwealth

Acknowledgements

This Act was drafted by Maxine L. Binns, Susan Jarvis and Loretta Joseph with valuable review by Yvan Jean-Louis. The drafting team was assisted by a team of industry experts: Kokila Alagh, Lt Col Keron Burrell, Stuart Davis, Alexandra Delsol, Paul Derham, Ankita Dhawan, Elizabeth Genia, Jonathan Hatch, Marc Krisjanous, Louise Malady, Ian Matthews, Rick McDonell, Harvesh Seegolam, Lord Anthony St John, Jane Thomason, Siddarth Tiwari, Muazu Umaru, Joseph Weinberg, Jeff Yew, Anson Zeall, Wei Zhou. Full biographies are available in the Annex.

The Model Law was developed with the support of Prof. Luis Franceschi (former Assistant Secretary-General, Commonwealth Secretariat) and Dr Elizabeth Macharia (Legal Adviser and Acting Head of Rule of Law, Commonwealth Secretariat).

The authors' knowledge and understanding of the regulation of stablecoins across the Commonwealth also benefited from a series of meetings with the Expert Working Group convened by the Commonwealth Secretariat and Chaired by Yvan Jean-Louis.

Introduction

The advent of stablecoins represents a pivotal evolution in global finance, redefining traditional concepts of currency, financial transactions and economic interaction. Recognising both the transformative potential and the inherent risks, the Commonwealth Secretariat introduces this Model Law on Stablecoins. This comprehensive regulatory framework aims to establish trust within the emerging digital financial ecosystem, enabling industry, customer and investor protection; providing for robust financial integrity; and ensuring the stability of economic systems across member countries.

The Commonwealth Model Law on Virtual Assets ("the principal Act") serves as the principal or umbrella legislation governing the regulation of Virtual Assets (**VAs**) and the entities that provide related services across member countries (Virtual Asset Service Providers, or **VASPs**, as defined in the principal Act). This foundational law establishes the baseline legal and regulatory framework for anti-money laundering/countering the financing of terrorism (AML/CFT) compliance, licensing, supervision and operational conduct of VASPs. Building upon the principal Act, this Model Law on Stablecoins ("the Model Law") acts as an extension – effectively a "Part II" of the VASP framework – specifically tailored to address the unique characteristics and systemic implications of stablecoins.

While anchored in the principles and obligations set out under the principal Act, this Model Law introduces its own comprehensive legal and regulatory framework, including distinct provisions for, among others, reserve management, disclosure, algorithmic mechanisms, and cross-border interoperability and corroboration between different networks.

This layered approach ensures coherence with the overarching VA regime while providing the specialised legal architecture necessary to effectively regulate stablecoins. In this regard, the Financial Action Task Force (**FATF**) has clarified that most stablecoins are considered VAs, particularly those not representing a legal tender fiat currency and those used for payments or trading. If a stablecoin does not qualify as a "financial asset" under another FATF definition (e.g., e-money, securities), it generally falls under the VA category. Accordingly, the activities surrounding stablecoins (issuance, transfer, exchange, custody, etc.) are subject to FATF Recommendations 15 and 16 and VASP obligations.

Aligned closely with the best practices set forth by the international standard-setting bodies, including the Financial Stability Board (**FSB**), the Bank for International Settlements (**BIS**), the Basel II framework, the International Organization of Securities Commissions (**IOSCO**) and FATF, the Model Law underscores the importance of transparent reserve asset management, rigorous governance standards and stringent transparency requirements to prevent systemic financial risks. It mandates that Stablecoin Issuers maintain reserves consisting of short-term High-Quality Liquid Assets to ensure stability and redemption certainty.

Although stablecoins are designed to maintain a stable value relative to a referenced asset, they share many of the same money laundering (**ML**), terrorism financing (**TF**) and proliferation financing (**PF**) risks associated with other VAs. As highlighted in FATF's report to the G20, these risks arise from features such as potential anonymity, cross-border functionality and the ability to facilitate the layering of illicit funds.

However, certain stablecoin arrangements may pose heightened risks as a result of their greater potential for mass adoption. This amplifies the relevance of treating the

Issuer or service provider as a "Financial Institution", which is defined as any entity that is licensed or authorised by a prudential or financial regulatory authority to engage in one or more financial activities as a business for the purposes of ML/TF/PF risk assessment. While the risk of widespread use applies broadly to all VAs, it is especially significant when evaluating the ML/TF/PF exposure risk stablecoins pose.

Stablecoins have characteristics that could overcome factors that have held back the widespread adoption of VAs as a means of payment. By maintaining a stable value, stablecoins are designed to overcome the price volatility issues sometimes associated with many VAs. Reduction of volatility could encourage their widespread use as a means of payment or transferring funds, particularly when they are sponsored by large technology, telecommunication or financial firms that could offer global payment arrangements.

Stablecoins can be centralised or decentralised, in terms of both their governance and who can access stablecoins (e.g., whether unhosted wallets are allowed or not, whether the system is permissioned or permissionless) and offer related services.

Stablecoin governance bodies will generally fall under FATF standards, either as VASPs or as FIs. When stablecoin arrangements involve higher levels of decentralisation, the associated risks must be mitigated through reserve-backed assets, in accordance with a country's broader obligations under FATF and any other internationally accepted regulatory standards. The risks should be identified and assessed before product launch and managed and mitigated in an ongoing and forward-looking manner.

This Model Law further emphasises the coexistence of public and private money in the digital age, recognising that, while central banks develop sovereign digital currencies (central bank digital currencies, **CBDCs**), privately issued stablecoins can complement these initiatives greatly. To foster this balance, the Model Law proposes a technology-neutral approach, ensuring adaptability and continuous relevance in the face of rapid technological advancements.

Recognising the importance of financial inclusion, especially within regions lacking robust traditional financial infrastructure, stablecoins offer substantial opportunities to enhance economic participation through accessible, cost-efficient financial services. Thus, the regulatory approach is designed to nurture innovation responsibly without compromising financial stability or industry, customer and investor protection.

Additional key stipulations incorporated into the Model Law include the following:

- clear regulatory classifications distinguishing between different classes of stablecoins, allowing for proportionate regulatory oversight;
- mandatory independent audits and transparency requirements to verify that stablecoin reserves adequately back the circulating supply; and
- promotion of cross-border regulatory co-ordination to prevent regulatory arbitrage and maintain international market integrity.

This Model Law represents the Commonwealth's proactive commitment to establishing a secure, innovative and inclusive digital financial future, setting a global benchmark for stablecoin governance and regulatory standards.

As a non-binding framework, it is offered to member countries for voluntary adoption. If any member country decides to use the provisions of this Model Law, the resulting law should be tailored according to their national priorities and existing legal framework, as well as their economic and institutional circumstances.

Principles

This Model Law is based on the following guiding principles—

(a) **Principle-Based:** The regulatory framework is principle-based and outcome-focused and offers sufficient flexibility to minimise its intrusiveness on innovation. It adopts a light-touch approach so as to support the development of new technologies rather than hinder it.

(b) **Protection-Focused:** The regulatory framework protects market participants from counterparty risks and covers market integrity, surveillance, fair pricing, custody, clearing, disclosure of conflicts of interest, and systems and business continuity planning.

(c) **Balanced and Proportionate:** The regulatory framework balances the need for regulation with the need for protection. It should be proportionate to allow innovative firms in the development stages to succeed while ensuring financial stability and financial integrity in the market.

(d) **Comprehensive:** The overall regulatory framework is comprehensive, and incorporates the entire ecosystem of web3 technologies and avoids an exclusive focus on VAs. Even if the Model Law is limited in scope, Commonwealth countries can align on the way forward in terms of the regulatory next steps.

(e) **Flexible and Adaptable:** The regulatory framework maintains technology-neutrality and flexibility and respects the varying levels of regulatory readiness and resources across Commonwealth member countries. It avoids prescribing administrative requirements and, wherever possible, member countries can customise the framework and supplement it through delegated legislation – such as, among others, implementing regulations, guidance, circulars, rules, codes and frequently asked questions (FAQs). It preserves the sovereignty of Commonwealth member countries and upholds their authority to legislate independently.

An Act to regulate entities involved in the issuance, transfer, custody, exchange or redemption of stablecoins; to empower the Regulatory Authority with oversight, investigatory and enforcement functions; and to provide for related and ancillary matters.

Explanatory Note:

The Long Title may vary as determined by each Commonwealth member country.

Part I
Preliminary

1. Short title

This Act may be cited as the Stablecoins Act [year].

> **Explanatory Note:**
>
> In section 1, each Commonwealth member country may choose to name the law differently. Alternatively, a Commonwealth member country may, instead of drafting a standalone law on stablecoins, choose to incorporate the provisions of this Model Law into existing laws or delegated legislation, including but not limited to laws governing VAs, financial services or AML/CFT, among others.

2. Interpretation

In this Act, the following words and expressions have the meanings assigned to them:

Algorithmic Stablecoin means a type of Stablecoin that seeks to maintain a stable value through the use of algorithms, smart contracts or protocol-defined rules that automatically adjust the supply or demand of the token – without direct backing by fiat currency, commodity reserves or other tangible assets and which may rely on mechanisms such as rebasing, seigniorage models or the use of volatile crypto-assets as collateral to stabilise prices.

Blockchain means a type of distributed ledger (**DLT**), consisting of a growing list of records, called blocks, that are securely linked together using cryptographic techniques, wherein each block contains a timestamp and a reference to the previous block, thereby forming a verifiable and immutable chain of information.

Compensation Fund means a fund designed to reimburse customers in the event of Issuer insolvency or fraud.

DAO means Decentralised Autonomous Organisation.

De-pegging means the loss or breakdown of the price stability mechanism of a Stablecoin, resulting in the coin trading at a material variance from its intended peg.

Distributed Ledger Technology (DLT) means a technological infrastructure and protocols that allow the decentralised recording, sharing and synchronisation of data across multiple nodes or participants in a network, without the need for a centralised data storage or administration.

Fiat Currency has the same meaning as defined in the principal Act.

Financial Institution means—

(a) any entity that is licensed or authorised by a prudential or financial Regulatory Authority to engage in one or more of the following activities as a business—
  (i) accepting deposits or other repayable funds from the public;
  (ii) providing credit or financing of any kind;
  (iii) providing money or value transfer services;
  (iv) issuing payment instruments, including electronic money or Stablecoins;
  (v) trading in money market instruments, foreign exchange, financial derivatives or securities;
  (vi) managing individual or collective investments, including VAs;

(vii) providing financial leasing, financial guarantees or commitments;

(viii) safekeeping or administration of assets, including custodial services;

(ix) participating in securities or derivatives markets; or

(x) any other financial activity designated by the Regulatory Authority;

(b) for the purposes of this Act, includes any other entity prescribed by regulation as a Financial Institution.

High-Quality Liquid Assets means assets that can be easily and quickly converted into cash with little or no loss of value. The term is primarily used in the context of the liquidity coverage ratio under the Basel III banking regulations, which require banks to hold enough High-Quality Liquid Assets to cover net cash outflows for 30 days in a stress scenario.

Interoperability means the ability for systems, including blockchains, to interact and transact seamlessly.

Issuer means a Person who issues Stablecoins as specified in section 4(3).

Legal Person has the same meaning as defined in the principal Act.

Natural Person has the same meaning as defined in the principal Act.

Oracle means a blockchain-based system or service that connects the Stablecoin Ecosystem to external data sources, enabling it to access and utilise information from the real world. An Oracle sources, verifies and communicates data originating outside the Stablecoin Ecosystem to be used by and for the Stablecoin processes.

Permitted Reserve Assets has the meaning as defined in section 18.

Person means any natural person, legal person, trust, partnership, unincorporated association, DAO or other body, entity or arrangement – whether or not possessing separate legal personality or legal capacity under applicable law.

Principal Act means the Commonwealth Model Law on Virtual Assets.

Regulatory Authority has the same meaning as in section 2(1)(k) of the principal Act and includes, for the purposes of this Act—

(a) a designated Prudential Authority responsible for supervising Tier 1 Issuers and other Financial Institutions engaged in systemic or wholesale Stablecoin Activities;

(b) the Securities Regulator, where Stablecoins are classified or offered as securities or investment products; and

(c) any other regulatory body designated by law or by the Minister to supervise Stablecoin Activities within their mandate.

Regulatory Impact Assessment means an analysis that evaluates the effect of new regulation on stakeholders and the economy.

Reserve means the pool of assets that an Issuer holds to back the value of the issued Stablecoin to ensure its stability relative to the referenced currency or asset.

Secure Coding means techniques used to prevent vulnerabilities in software design and implementation.

Segregated Account means a custodial or trust account in which customer funds are held separately from the Issuer's own assets and cannot be commingled or used for proprietary purposes.

Smart Contract means a self-executing contract with the terms of the agreement directly written into code and thereby manages the issuance, redemption and transactions of Stablecoins.

Smart Contract Custom Software Code means the programming code that defines the behaviour and rules of the Smart Contract, and that specifies the conditions under which Stablecoins can be issued, transferred or redeemed.

Stablecoin has the same meaning as in section 6.

Stablecoin Activities has the same meaning as in section 9.

Stablecoin Ecosystem means the interconnected components, participants and applications that are involved in the creation, management and use of Stablecoins.

Stablecoin Issuance means the making of a Stablecoin publicly available for purchase or acquisition by an Issuer.

Tier 1 has the same meaning as in section 14(1)(a).

Tier 2 has the same meaning as in section 14(1)(b).

Tier 3 has the same meaning as in section 14(1)(c).

Tiered Licensing Framework means a risk-based approach where licensing requirements differ based on the scale of issuance, the type of Stablecoin issued, the risk exposure (AML/CFT, market stability and technological resilience) and the nature of the issuing entity.

User refers to an individual or entity that acquires, holds, transfers or redeems Stablecoins for personal, commercial or institutional purposes, but who is not acting as an Issuer.

Virtual Assets (VAs) has the same meaning as defined in the principal Act.

Virtual Asset Service Provider (VASP) has the same meaning as defined in the principal Act.

White Paper has the same meaning as defined in the principal Act.

Explanatory Note:

The definitions contained in section 2 of this Model Law and the principal Act are indicative. Commonwealth member countries may include more defined terms.

The acronyms for global standard-setting bodies are as follows, for ease of reference:

FATF means Financial Action Task Force

IOSCO means International Organization of Securities Commissions

FSB means Financial Stability Board

IMF means International Monetary Fund

BIS means Bank for International Settlements

OECD means the Organisation for Economic Co-operation and Development

3. Objects of this Act

In addition to the objects of the principal Act, the objects of this Act are to specifically—

(a) establish a harmonised and interoperable legal and regulatory framework for Stablecoin issuance, use and supervision that operates in tandem with the principal Act;

(b) ensure financial stability and compliance with global standards;

(c) promote trust in the financial system through commercial, customer and investor protection;

(d) promote responsible innovation, global interoperability and cross-border co-operation;

(e) encourage the adoption of Stablecoins as a financial inclusion tool;

(f) enhance transparency and increase efficiency in evolving payment systems; and

(g) potentially reduce costs associated with financial transactions.

4. Scope and Application of Act

(1) This Act applies to an Issuer and User of Stablecoins in [*insert name of Commonwealth member country*] that engages in providing a VA service that includes Stablecoin Activities.

(2) This Act governs both retail and wholesale Stablecoins, including those used for—

  (a) domestic cross-border transactions;

  (b) clearing and settlements;

  (c) programmability; and

  (d) embedded or automated financial functions (e.g., lending, staking and insurance features).

(3) Stablecoins may only be issued, governed or managed by—

  (a) Issuers of VAs that meet the licensing requirements and obligations set out in this Act and the principal Act; and

  (b) any other authorised entities, including—

    (i) DAOs;

    (ii) entities issuing algorithmic, rebase or protocol-native Stablecoins; or

    (iii) entities that manage Stablecoins designed to maintain value stability through decentralised or non-traditional mechanisms, including price oracles, algorithmic market operations or autonomous Smart Contracts or hybrid structures provided they are authorised by the Regulatory Authority.

(4) For the purpose of this Act, the entities identified in 4(3)(a) and (b) are referred to as "Stablecoin Issuers" or "Issuers," and both terms are used interchangeably.

(5) For the purposes of this section, "intermediary" means any Person or entity that facilitates the issuance, distribution, exchange, custody or redemption of Stablecoins on behalf of an Issuer or user, including but not limited to digital asset exchanges, wallet providers, custodians and payment processors.

Explanatory Note:

Section 4 defines the scope of application of the Act and sets out who may lawfully issue Stablecoins within the relevant Commonwealth member country. It applies to both centralised and decentralised actors, including DAOs (e.g., MakerDAO) and artificial intelligence (**AI**)-driven protocols developing algorithmic or autonomous Stablecoin models.

In the case of DAO, however, FATF does not currently provide a single, formal definition of a DAO in its glossary but its guidance on VAs and VASPs does touch upon DAOs in the context of AML/CFT obligations and, in practice, tends to treat DAOs as potential VASPs if they are involved in activities such as exchanging, transferring or safekeeping VAs. This means that, even if a DAO is governed by code and lacks a traditional corporate structure, it may still fall under FATF's regulatory scope if it performs functions similar to those of a financial intermediary.

Algorithmic Stablecoin Risk Warning: Owing to their reliance on market incentives, assumptions of rational user behaviour and potential vulnerabilities in algorithmic design, Algorithmic Stablecoins are generally considered to pose higher financial, operational and systemic risks. These may include risks of de-pegging, liquidity collapse or cascading failure during periods of market stress. Regulatory Authorities should assess such Stablecoins with heightened scrutiny and may impose additional prudential and disclosure requirements, including Tier 3 classification under this Act.

By expressly including retail, wholesale, programmable and cross-border uses, the Act ensures the legal framework accommodates both traditional Financial Institutions and Decentralised Finance (DeFi) applications. The inclusion of AI-generated and autonomously managed Stablecoins reflects an anticipatory regulatory stance on emerging technologies.

Generally, Part I sets the legislative foundation by outlining the title, objectives, scope and key concepts. It aligns with the principal Act to ensure regulatory consistency and interoperability. The objectives emphasise financial stability, customer protection, innovation and cross-border co-operation, reflecting the need for a harmonised yet flexible legal framework.

Standard-Setter References:

- FATF Recommendation 15 – includes decentralised Issuers and requires AML/CFT compliance
- IOSCO Crypto-Asset Roadmap (2020–2023) – addresses governance and systemic implications of Stablecoins
- BIS Committee on Payments and Market Infrastructures – emphasises programmable, cross-border potential
- FSB High-Level Recommendations (2020–2023) – supports inclusion of decentralised and algorithmic models

5. Objectives of the Regulatory Authority

(1) The objectives and functions of the Regulatory Authority as set out in Part II of the principal Act are incorporated by reference in this Act.

(2) To the extent of inconsistency, this Act prevails over the principal Act in relation specifically to the regulation of Stablecoin Issuers.

Part II
Regulation of Stablecoin Issuance and Related Activities

6. The Definition of Stablecoins

(1) For the purposes of this Act, a Stablecoin refers to a class of VAs designed to maintain a stable value by referencing the value of one or more assets, including official currencies, commodities or other financial instruments, which is transferable electronically using DLT and which functions as a store of value, unit of account or medium of exchange.

(2) Stablecoins may be classified into the following categories, with each category subject to distinct licensing and regulatory requirements—

(a) Payment Stablecoins that aim to maintain a stable value by referencing a single official currency and redeemable at par value;

(b) Reserve-backed Stablecoins that reference a combination of VAs, including but not limited to fiat currencies, commodities or other financial instruments;

(c) Yield-bearing Stablecoins that reference any mechanism embedded in the Stablecoin or offered by the Issuer enabling the holder to receive income, interest or rewards in return for holding, staking or locking the Stablecoin, whether such returns are fixed, variable or algorithmically determined.

(3) The Regulatory Authority may do either or both of the following pertaining to Stablecoins—

(a) specify a unit of account or store of economic value;

(b) specify a digital representation of value or class of digital representations of value.

7. Regulated Stablecoin Issuance

(1) A Legal Person must not issue a Stablecoin unless authorised by the Regulatory Authority in accordance with Part V of the principal Act or under the provisions of this Act and any related regulations.

(2) Subject to section (1), a Stablecoin may be issued by—

(a) minting a digital token on a distributed ledger network and assigning it to a user account; or

(b) any other approved issuance mechanism authorised by the Regulatory Authority.

(3) The Issuer must maintain accurate, real-time records of all issuance, distribution and redemption transactions of Stablecoins, and provide such records to the Authority upon request.

Explanatory Note:

Stablecoin Issuance is the process by which a Legal Person creates and places into circulation a Stablecoin in exchange for fiat currency or other assets, with a promise or mechanism to redeem that Stablecoin for the underlying value. Issuance may occur through direct sale, algorithmic mechanism or collateralisation, and must comply with licensing, reserve and disclosure requirements as specified under this Law. Issuers are responsible for ensuring redeemability, maintaining adequate reserves and complying with prudential and conduct standards.

(4) The issuance of Stablecoins with yield-bearing features will be subject to additional or enhanced disclosure, transparency and risk management obligations as prescribed by the Regulatory Authority, including the clear identification of—

(a) the source of yield generation;

(b) the Issuers responsible for yield distribution;

(c) any contractual or algorithmic mechanisms governing the yield; and

(d) any associated risks of loss, volatility, or de-pegging.

Explanatory Note:

This section allows Regulators to treat yield-bearing Stablecoins as regular Stablecoins with an added risk or functionality. It provides flexibility for the law to cover innovations like staking rewards, DeFi integration or tokenised interest accounts without needing to define an entirely new class of VAs.

8. Prohibition on Stablecoin Issuers

A Natural Person:

(a) must not offer or issue Stablecoins as a business in [*insert name of Commonwealth member country*]; and

(b) must not issue Stablecoins in [*insert name of Commonwealth member country*] except in accordance with this Act.

9. Regulated Stablecoin Activities

(1) A Legal Person must not carry on, or purport to carry on, any Stablecoin Activity unless that Legal Person is—

(a) duly authorised, registered or licensed under this Act or the principal Act; and

(b) in compliance with any conditions imposed by the Regulatory Authority.

(2) For the purposes of this Act, a Legal Person carries on a regulated Stablecoin Activity if it—

(a) issues a Stablecoin in the course of business;

(b) issues a Stablecoin in any location in the course of business, and the Stablecoin purports to maintain a stable value with reference to a specific currency or basket of assets;

(c) carries on an activity specified under section 10(3); or

(d) offers or facilitates yield-bearing features on Stablecoins, including through protocols, platforms or service providers, that constitute a regulated activity under this Act and requires prior authorisation.

(3) A reference to a regulated Stablecoin Activity is to be construed accordingly and as prescribed by section 8 of the principal Act.

(4) This section also applies to DAO-issued and niche Stablecoin—

(a) issued, governed or managed by a DAO;

(b) structured as an algorithmic, rebase or protocol-native Stablecoin;

(c) designed to maintain value stability through decentralised or non-traditional mechanisms, including price oracles, algorithmic market operations or autonomous smart contracts.

(5) DAO-issued or niche Stablecoins will be subject to the applicable Tier classification and supervision under this Act, unless explicitly exempted by the Regulatory Authority.

(6) Subject to subsection (7), a DAO or decentralised protocol will not be exempt from regulatory obligations on the basis of its structure alone.

(7) Where there is no identifiable Legal Person, the DAO must appoint a responsible person, compliance agent or legal representative with authority to interface with the Regulatory Authority.

Explanatory Note:

This section refers to "Stablecoin Activities" as the full range of functions involved in issuing and managing stablecoins – including token creation, reserve management, transaction processing, governance, third-party arrangements and disclosure obligations. It clarifies that this broad definition enables Regulators to oversee all critical functions, including decentralised or cross-border models, ensuring comprehensive compliance and consumer protection.

For the purposes of section 9(4), a niche Stablecoin typically refers to a Stablecoin designed for a specialised use case, community or market segment, rather than broad, general-purpose adoption.

10. Carrying on Regulated Stablecoin Business

(1) For the purposes of this section, a person carries on Stablecoin business if they engage in any activity involving the issuance, redemption, reserve management, custody or operation of Stablecoins, whether as principal, agent or service provider.

(2) For the purposes of this Act, section 2(1)(m)(v) of the principal Act applies to carrying on regulated Stablecoin Activities as a VASP, if—

(a) any Issuer actively markets, whether domestically or internationally, to the public that such Issuer carries on, or purports to carry on, such activity; and

(b) the activity, if carried on within a regulated financial framework, would constitute a regulated Stablecoin Activity.

(3) Subsection (1) applies in relation to an Issuer regardless of—

(a) whether the carrying on, or purported carrying on, of an activity mentioned in subsection (2)(a) is actively marketed by the Issuer or another Person on behalf of the Issuer; and

(b) whether the activity mentioned in section 9(2)(a) is carried on or not.

(4) The Regulatory Authority may, after consulting relevant financial authorities, specify an activity for the purposes of section 9.

(5) In exercising a power to specify an activity under subsection (4), the Regulatory Authority must, in addition to any other matters that the Authority considers relevant, have regard to—

(a) whether the activity is, or is likely to become, material to the monetary or financial stability of [*insert name of Commonwealth member country*];

(b) whether the activity is, or is likely to become, material to the functioning of [*insert name of Commonwealth member country*] as a financial centre; and

(c) the matters of significant public interest, including but not limited to—

(i) the protection of customers, investors or end-users of Stablecoin systems;

(ii) the prevention of financial crime, including money laundering, terrorist financing and proliferation financing;

(iii) systemic risks arising from market concentration, technological failure or governance weaknesses;

(iv) the promotion of competition, innovation and financial inclusion; and

(v) the upholding of public trust and confidence in the digital financial system.

(6) For the purposes of subsection (5)(a), an activity is or is likely to become material to monetary or financial stability if the occurrence of any significant disruption to the carrying on of the activity is likely to adversely affect financial system stability.

(7) For the purposes of subsection (5)(b), an activity is or is likely to become material to the functioning of a financial centre if the occurrence of any significant disruption to the carrying on of the activity is likely to—

(a) adversely affect the role of [*insert name of Commonwealth member country*] as a financial centre; or

(b) cause systemic disruption to the financial system.

(8) For the purposes of subsection (5)(c), the following matters are to be regarded as matters of significant public interest—

(a) whether the occurrence of any significant disruption to the carrying on of the activity is likely to adversely affect the public's confidence in the financial system; and

(b) whether the occurrence of any significant disruption to the carrying on of the activity is likely to adversely affect day-to-day commercial activities.

Explanatory Note:

This section sets out the foundational requirement that persons engaged in Stablecoin Activities must be duly authorised or registered under the relevant legal framework. It clarifies that operating a Stablecoin business constitutes a regulated financial service, particularly where such activities involve the issuance, redemption, reserve management or custody of assets on behalf of customers.

By requiring formal authorisation, the provision ensures such activities are conducted in accordance with prudential, consumer protection and anti-financial crime standards, and fall within the scope of supervisory oversight. This obligation supports legal certainty, market stability and trust in digital financial instruments, and reflects international best practices in regulating payment-related digital asset services.

Part III
Licensing and Authorisation

11. Licensing Required for Stablecoin Issuers

(1) A Person must not issue, or hold themselves out as issuing, Stablecoins unless that Person—

(a) is duly licensed as a Stablecoin Issuer under this Act or the principal Act; and

(b) complies with all applicable conditions imposed by the Regulatory Authority.

(2) To apply for a Stablecoin Issuer licence, the applicant must be an entity registered or licensed in [*insert name of Commonwealth member country*] or an authorised Issuer incorporated outside [*insert name of Commonwealth member country*].

(3) An application for a licence to carry on business as an Issuer must be in the form prescribed by the Regulatory Authority in regulations.

(4) The Regulatory Authority may grant a licence to an applicant if it is satisfied that—

(a) the applicant is fit and proper to carry on Stablecoin Activities;

(b) appropriate arrangements are in place for reserve management, governance, risk control and customer protection; and

(c) the applicant meets any financial, technological, and operational criteria prescribed by rules or directives.

(5) The Regulatory Authority may prescribe by rules—

(a) classes or tiers of Stablecoin licences;

(b) exemptions or modifications for experimental, limited scale or sandbox activities; and

(c) procedures for application, renewal, suspension or revocation of licences.

(6) Any Issuer that is licensed in [*insert name of Commonwealth member country*] or a country that is deemed by the Regulatory Authority to be equivalent in substance and effect to the requirements under the principal Act and this Act may apply for a registration in [*insert name of Commonwealth member country*] in order to offer its services or Stablecoins to residents and/or nationals of [*insert name of Commonwealth member country*].

Explanatory Note:

This section mandates that each Commonwealth member country may, through its own laws and regulatory procedures, adopt a similar or simplified registration process for such entities, as appropriate. Only entities licensed by the Regulatory Authority may issue Stablecoins. The section ensures Issuers meet key standards for governance, financial soundness and consumer protection. The Model Law supports market integrity by enabling tailored licensing, including tiered regimes and sandbox options, while promoting responsible innovation and supervisory oversight.

12. Obligations for Licensed Stablecoin Issuers

(1) A person licensed as a Stablecoin Issuer under this Act must conduct its Stablecoin Activities in a manner that promotes financial integrity, customer protection and systemic stability.

(2) Issuers must comply with the obligations set out in Parts III and IV of the principal Act and under the provisions of this Act.

(3) A licensed Stablecoin Issuer must, in addition to subsection (2)—

(a) comply with the obligations imposed on Issuers of Initial VA Offerings as set out in section 31 of the principal Act;

(b) operate as fiduciaries with respect to customer holdings and act in the best interest of Stablecoin holders, prioritising the protection, safekeeping and liquidity of reserve assets;

(c) treat customers equally;

(d) include in its White Paper key information including the information provided for in Exhibit E;

(e) publicly disclose guidelines on implementation timelines issued for Issuers by the Regulatory Authority; and

(f) meet the reserve management and transparency obligations set forth under Part IV.

Explanatory Note:

This section sets out the core obligations for licensed Stablecoin Issuers establishing a high standard of conduct, transparency and operational integrity.

This Model Law reinforces compliance with key legal obligations while enhancing Stablecoin Issuer accountability. It establishes—

(a) regulatory alignment: ensuring coherence with broader VA laws, covering Issuer obligations and risk disclosures;

(b) fiduciary standards: mandating that Issuers act in holders' best interests, similar to traditional finance trustees;

(c) fairness and inclusion: guaranteeing non-discriminatory treatment, supporting cross-border financial accessibility;

(d) transparency in White Papers: requiring clear, accessible disclosures on price stability and redemption rights;

(e) regulatory accountability: Issuers must publish implementation timelines and milestones, promoting predictable compliance; and

(f) reserve and audit requirements: linking Issuer obligations to segregated reserves, independent audits, and reporting to ensure stability.

Collectively, these obligations are designed to reinforce trust in Stablecoin arrangements, support sound governance and mitigate financial and operational risks. They provide the legal foundation for supervisory enforcement and stakeholder recourse in the event of mismanagement or misconduct by Issuers.

13. Tiered Licensing Framework for Licensed Stablecoin Issuers

(1) The Regulatory Authority may implement a tiered licensing framework for licensed Stablecoin Issuers, based on risk exposure and systemic importance.

(2) Tier 1 Issuers may be identified by the following characteristics—
  (a) significant market reach and financial system implications;
  (b) minimum quantitative thresholds as set out in Exhibit A; and
  (c) significant cross-border operations.

(3) Tier 1 Issuers may be subject to a full range of prudential, governance, disclosure and cross-border supervisory standards.

(4) Tier 2 Issuers may be identified by the following characteristics—
  (a) Issuers of moderate-scale Stablecoins; and
  (b) minimum quantitative thresholds as set out in Exhibit A.

(5) Tier 2 Issuers may be required to meet baseline capital, reserve, AML/CFT and governance standards.

(6) Tier 3 Issuers may be identified by the following characteristics—
  (a) issuers for closed-loop Stablecoin Ecosystems;
  (b) limited use cases; and
  (c) minimum quantitative thresholds as set out in Exhibit A.

(7) Tier 3 Issuers may be subject to simplified licensing with AML/CFT, customer protection and information technology security obligations.

(8) The duration of a licence issued to a Tier 1, 2 or 3 Issuer will be subject to the discretion of the Regulatory Authority.

(9) Tier 0 Issuers may be identified by the following characteristics—
  (a) Issuers operating under a regulatory sandbox or a DAO with capped issuance; and
  (b) minimum quantitative thresholds as set out in Exhibit A.

(10) The duration of a licence issued to a Tier 0 Issuer is twelve (12) months and may only be renewed once.

Explanatory Note:

This section introduces a risk-based licensing regime that enables the Regulatory Authority to differentiate requirements based on the scale, systemic importance and operational complexity of Stablecoin Issuers. The tiered approach may be customised by each Commonwealth member country to ensure regulatory obligations are proportionate, promoting innovation and market entry while preserving financial stability and user protection.

Higher tiers may be subject to more stringent requirements – such as enhanced reserve obligations, reporting standards and supervisory oversight – where Issuers pose greater systemic or cross-border risk. Conversely, lower tiers or sandbox regimes may allow for limited-scale operations with graduated compliance.

This framework enhances regulatory flexibility, encourages responsible innovation and aligns with international best practices for supervising emerging digital asset markets.

14. Tiered Regulatory Classification and Oversight Responsibilities

(1) For the purposes of licensing and regulatory supervision of Issuers under the principal Act and this Act, such Issuers may be classified into the following tiers based on their size, systemic importance, risk exposure and issuance model, as appropriate.

(2) Tier 1 Classification includes Financial Institutions or entities whose Stablecoin Activities are systemically important, including those—
  (a) with high transaction volume or customer base;
  (b) with wholesale, cross-border or interbank use cases; or
  (c) whose failure would pose a material threat to financial stability.

(3) Where the Financial Institutions or entities fall within the Tier 1 classification, the Regulatory Authority may be the Prudential Regulator.

(4) Tier 2 Classification includes regulated VASPs and Financial Institutions offering Stablecoin services to retail or institutional customers at scale, but without systemic impact, and includes—
  (a) non-bank Financial Institutions;
  (b) regulated VASPs, payment service providers or e-money institutions;
  (c) custodial Stablecoin Issuers.

(5) Where the entity falls within the Tier 2 classification, the Regulatory Authority may be either the Securities Regulator (or VASP Supervisor) or the Prudential Regulator.

(6) Tier 3 Classification includes limited or niche Issuers or entities issuing Stablecoins with limited scope or experimental use, including—
  (a) pilot or sandbox programmes;
  (b) Algorithmic Issuers or DAOs with capped issuance or user thresholds;
  (c) community or niche use cases.

Explanatory Note:

This section empowers the Regulatory Authority to accommodate innovation through a sandbox or conditional regime, ensuring balanced innovation and customer protection. Including an innovation safe harbour for decentralised Stablecoins in this Model Law can foster responsible growth and experimentation while mitigating risks. It establishes—

(1) an environment that encourages innovation: allows developers to test new decentralised Stablecoin models without immediate regulatory constraints, fostering creativity and technological advancement;

(2) regulatory clarity: provides a structured framework for emerging Stablecoin projects, ensuring compliance while avoiding premature restrictions that could stifle development;

(3) customer protection: creating safeguards within the safe harbour ensures users are protected from fraud, mismanagement or unexpected failures;

(4) market stability: by allowing controlled experimentation, regulators can assess risks and refine policies before full-scale implementation; and

(5) global competitiveness: countries that adopt innovation-friendly policies can position themselves as leaders in the digital asset space, attracting investment and talent.

For the purposes of section 14(3), the Prudential Regulator may be the Central Bank or Financial Stability Oversight Authority.

(7) For the purposes of subsection (6)(b), Algorithmic Stablecoins:
  (a) must be assessed by the Regulatory Authority and, unless otherwise demonstrated to have equivalent reserve and stabilisation mechanisms, may default to Tier 3 classification to operate under a conditional licence;
  (b) relying solely on endogenous assets may be disallowed by default unless expressly permitted and explicitly require enhanced obligations.

(8) Issuers of Algorithmic Stablecoins must meet enhanced obligations under this Act, including but not limited to—
  (a) disclosure of algorithmic mechanisms and failure scenarios;
  (b) independent code audit and stress testing;
  (c) contingency plans for market volatility and de-pegging events;
  (d) reserve buffers, if hybrid collateral models are used;
  (e) enhanced investor risk disclosures; and
  (f) any other obligations that the Regulatory Authority may deem fit.

Explanatory Note:

These measures are necessary to mitigate the elevated risks posed by algorithmic structures, which lack conventional collateral and have historically demonstrated susceptibility to systemic failure.

For the sake of 7(b), endogenous assets include for example:

UST was an **algorithmic stablecoin** designed to maintain a 1:1 peg with the US dollar. **LUNA** was its **balancing token**, used to absorb volatility and maintain the peg through a mint-and-burn mechanism.

(9) DAO-issued Stablecoins will be classified as Tier 3 Stablecoins unless the Issuer can demonstrate to the satisfaction of the Regulatory Authority—
  (a) the existence of verifiable, transparent governance structures;
  (b) the appointment of one or more identifiable responsible persons for compliance;
  (c) implementation of multi-signature or M-of-N control systems over treasury and protocol changes;
  (d) periodic independent audits of reserve assets and Smart Contracts; and
  (e) the ability to meet reserve, redemption and disclosure requirements under this Act.

(10) Where a DAO-issued Stablecoin is unable to meet the requirements of this Act, the Regulatory Authority may prohibit its issuance, promotion or access through regulated VASPs in [*insert name of Commonwealth member country*].

Explanatory Note:

Section 14(6) establishes a default Tier 3 classification for licensing and regulatory supervision owing to higher inherent risk, while providing a pathway for DAOs to demonstrate equivalence to traditional Issuers.

In section 14(9)(c) M-of-N refers to a cryptographic or operational control mechanism whereby a minimum number (M) of authorised parties or credentials, out of a total number (N), are required to approve, access or execute a sensitive operation or function to ensure fewer than M participants cannot successfully perform the operation.

(11) The Regulatory Authority may, by public notice—

(a) permit DAO-issued or algorithmic Stablecoins to operate under a conditional licence or within a regulatory sandbox;

(b) impose enhanced disclosure, AML/CFT screening and customer protection requirements; and

(c) require real-time monitoring and reporting and restrict retail access where appropriate.

(12) Where an entity falls within the Tier 3 classification, the Regulatory Authority may be either—

(a) the VASP supervisor;

(b) [Name of Innovation Unit]; or

(c) [Name of Special Regulatory Sandbox Framework].

(13) The Regulatory Authority must establish protocols for joint supervision and information-sharing, particularly where an Issuer meets multiple tier criteria or evolves across tiers.

Explanatory Note:

Commonwealth member countries may consider setting up innovation cells and sandbox frameworks for enabling the growth of Stablecoins.

Further, where functions across Regulators overlap, the relevant authorities must co-operate and co-ordinate in accordance with any memoranda of understanding or joint regulatory protocols to avoid duplication and ensure efficient supervision and issue the relevant guidance for the purposes of subsection (13).

(14) Issuers may be subject to reclassification by the Regulatory Authority based on periodic risk assessments, market activity or breaches of systemic thresholds, subject to appeal and transition rules under section 15(3).

(15) The Regulatory Authority may amend the tiered licensing framework from time to time by adding new tiers or amending the description of tiers as it considers necessary.

Explanatory Note:

In general, this section defines the supervisory responsibility of each tier of Issuers. The approach is consistent with FSB's recommendations for proportionate and risk-based regulation, FATF Recommendation 15 and risk classification of VASPs, IOSCO's Stablecoin Conduct Standards and the BIS–FSB framework on systemically important Stablecoin arrangements—

(a) Tier 1 oversight is aligned with global principles that systemic digital financial services must be regulated as prudentially significant entities (e.g., Basel III prudential rules, FSB Global Systemically Important Banks, **G-SIB**, standards).

(b) Tier 2 recognises the hybrid nature of many VASPs who may fall under securities, payments or e-money regimes depending on their business model, and thus regulatory oversight may lie with either the Securities Regulator (e.g., in the EU's Markets in Crypto-Assets, **MiCA**, Regulation or the UK's Financial Conduct Authority, **FCA**) or the Prudential Regulator (e.g., Monetary Authority of Singapore, **MAS**, Hong Kong Monetary Authority, **HKMA**).

(c) Tier 3 follows global trends on sandbox-friendly frameworks for innovation (e.g., UK FCA sandbox, Singapore's Project Orchid) and may be overseen by a fintech or innovation desk with bespoke conditions.

This classification ensures regulatory burden scales with systemic risk, prevents regulatory arbitrage and supports supervisory clarity across multiple sectors.

The appropriate place to integrate the provision defining the distinction between Stablecoin Issuer tiers and their corresponding Regulatory Authority (prudential or securities regulator) is directly after section 13 – "Tiered Licensing Framework for Licensed Stablecoin Issuers", as—

(a) Section 13 establishes the core tier classification system (Tiers 0–3);

(b) Section 14 elaborates the supervisory responsibilities for each tier, which provides essential institutional clarity that supports the licensing framework;

(c) Section 15 covers inter-tier transitions; and

(d) It bridges the tiered classification system with regulatory enforcement and jurisdictional clarity, something not yet clearly specified in section 13.

15. Inter-Tier Transition and Reclassification

(1) Issuers must monitor thresholds quarterly and notify regulators within 30 (thirty) days of nearing a higher tier.

(2) Issuers that temporarily exceed the transaction volume, reserve size or user base thresholds applicable to their current licensing tier must—

(a) notify the Regulatory Authority upon identifying a breach or the risk of a breach;

(b) indicate to the Regulatory Authority whether the breach was incidental and reversible and submit a remediation plan within five (5) business days of the breach;

(c) cease any further expansion of operations beyond the licensed limits until the Regulatory Authority approves either a return to compliance or a progression to a higher tier.

(3) Where a formal transition to a higher tier is intended, Issuers must indicate that intention to the Regulatory Authority and submit a transition plan within five (5) business days of indicating such intention.

(4) Issuers must incorporate in their business continuity plans reasonable forecasting and escalation procedures for potential tier breaches, including contingency for rapid compliance with higher-tier regulatory obligations.

(5) Issuers must submit reclassification documentation if [80 per cent] of a higher-tier threshold is reached.

(6) The Regulatory Authority may reclassify Issuers up or down and conduct reassessment within [sixty (60) days].

(7) The Regulatory Authority may apply provisional tier status during reclassification with temporary compliance flexibility.

Explanatory Note:

This section reflects regulatory practices such as those of Prudential Regulators, which expect regulated entities to proactively manage the risk of exceeding their authorised scope. Temporary breaches, especially those occurring near reporting cut-offs (e.g., month-end), may occur in growing businesses. Rather than automatic penalisation, this framework emphasises prudent forecasting, transparent reporting and operational pause mechanisms to uphold licensing integrity while enabling scalable innovation. Further, Commonwealth member countries may adjust the values and thresholds to best suit the context of their domestic economy.

This section also draws on cross-border enforcement themes from the principal Act, adapting them to account for systemic Stablecoin operations.

Key Concepts:

This framework may be operationalised through mechanisms such as regulatory sandboxes, supervisory no-action relief or graduated enforcement protocols that support innovation while maintaining market integrity. Member countries may apply proportionate supervisory responses based on the severity, recurrence, and systemic impact of any breaches:

(a) Regulatory Sandbox: A controlled environment where companies with new technologies can test innovations under limited regulatory environments, with regulatory support and supervision.

(b) Proportionate Sanctions: Penalties tailored to the scale and nature of the non-compliance.

Standard-Setter Reference:

- IMF/World Bank – stress the importance of cross-border supervisory co-operation

16. Fit and Proper Requirements and Tiered Approach to Prudential Standards

(1) The Regulatory Authority must assess the fitness and propriety of applicants and licensees in accordance with criteria set out in the principal Act and this Act or any regulations made thereunder.

(2) The Regulatory Authority may apply a tiered approach to prudential requirements, in accordance with the classification of Issuers under section 13, ensuring that—

(a) entities with systemic or large-scale operations are subject to enhanced prudential obligations; and

(b) smaller or niche Issuers are not subject to disproportionate regulatory burdens, while maintaining minimum standards of competence, integrity and compliance.

Explanatory Note:

This section establishes the legal foundation for the assessment of fitness and propriety of key Persons involved in the Stablecoin Ecosystem. It ensures that only competent, responsible and compliant individuals and entities are permitted to engage in issuance or related activities. The tiered regulatory approach balances the need for innovation and financial inclusion with the imperative of mitigating systemic risks.

By calibrating obligations according to the size, scale and risk profile of Issuers, the Model Law avoids overburdening smaller operators while ensuring robust safeguards for entities with greater market impact.

This Part aligns with the licensing sections in the principal Act expanding them to address Stablecoin-specific risks like reserve management and market impact.

Key Concepts:

(a) Tiered Licensing: A risk-based approach where the extent of regulation depends on systemic impact and scale of operations.

(b) Fit and Proper: A test of integrity, competence and financial soundness for owners and key personnel.

Standard-Setter References:

- FATF R.15 requires licensing or registration of VASPs
- FIMF: recommendations on proportional regulation for fintech and digital issuers
- FFSB (2023) Framework for International Regulation of Crypto-Asset Activities.

Part IV
Reserve Management and Transparency

17. Obligation to Maintain Reserves

(1) A licensed Stablecoin Issuer must at all times maintain reserve assets that are sufficient to meet all outstanding redemption obligations in respect of issued Stablecoins.

(2) The reserves referred to in subsection (1) must comprise only High-Quality Liquid Assets or cash equivalent that are prescribed under this Act or as may be approved by the Regulatory Authority.

Explanatory Note:

This section builds on prudential standards referenced in the principal Act by creating a robust reserve framework essential to how Stablecoin regimes manage financial integrity and market confidence.

The obligation to maintain reserves is a broader and more structural requirement. It focuses on continuity – mandating that reserve assets must be held at all times, not just at periodic audits or reporting intervals. This section ensures day-to-day solvency and reduces the risk of redemptions outpacing liquid backing.

Standard-Setter References:

- IOSCO-FSB (2023) – recommendations for reserve asset backing of Stablecoins
- BIS – supervisory and oversight expectations on stablecoin reserve management

18. Permitted Reserve Assets

(1) Permitted reserve assets are the specific types of assets that a Stablecoin Issuer is legally allowed to hold to back the value of its issued tokens, and are typically defined by regulation to ensure liquidity, stability and minimal credit risk.

(2) Permitted reserve assets must include—

(a) fiat currency held in deposit accounts with regulated financial institutions;

(b) government securities rated AA or higher, with a remaining maturity not exceeding ninety (90) days;

(c) units or shares in public money market funds investing in government debt securities and short-term cash deposits in commercial banks subject to Regulatory Authority-agreed limits, credit ratings and legal arrangements;

(d) other High-Quality Liquid Assets as may be approved by the Regulatory Authority, subject to liquidity and concentration requirements.

(3) Permitted reserve assets must not include—

(a) corporate equities;

(b) VAs;

(c) any asset issued by a related party;

(d) illiquid or encumbered instruments;

(e) any other assets determined by the Regulatory Authority.

Explanatory Note:

This section clarifies that the list of assets in section 18 is illustrative, not exhaustive, and that Commonwealth member countries may expand it based on local considerations.

It distinguishes reserve assets – a broad class of liquid, macroeconomic instruments used to support currency value – from permitted reserve assets, which are specifically authorised by law for use by Stablecoin Issuers. The latter are a constrained subset, selected to ensure safety, liquidity and redemption reliability.

Frameworks like the US Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act exemplify this by limiting permitted reserves to low-risk instruments such as central bank deposits, short-term treasuries and insured bank holdings.

The overarching aim is to ensure full and reliable redemption, even in times of market stress. Regulatory flexibility allows each Commonwealth member country to tailor its permitted list to its risk tolerance and policy goals.

19. Custody and Segregation of Reserves

(1) Reserve assets must be held—

(a) subject to subsection (3), in Segregated Accounts separate from corporate or operational funds; or

(b) in Financial Institutions that meet minimum capital adequacy and custody requirements set by the Regulatory Authority.

(2) Issuers must ensure reserve assets are legally protected from claims by creditors of the Issuer in the event of insolvency.

(3) Reserve assets held in Segregated Accounts are held on trust for the benefit of the holder of the Stablecoins.

Explanatory Note:

This section outlines the importance of segregating reserve assets to ensure bankruptcy protection. It mandates legal and structural safeguards – such as segregated accounts – to insulate user funds from Issuer insolvency or misconduct. By keeping reserves separate, recorded and properly safeguarded, the assets remain bankruptcy-remote, meaning neither the Issuer's creditors nor those of the custodian can claim them. Additionally, the value of these backing assets must remain independent of the Issuer's credit risk, reinforcing asset protection and user confidence.

20. Reconciliation and Redemption

(1) A licensed Stablecoin Issuer must implement systems and controls to ensure the number of issued Stablecoins is continuously reconciled against the value and availability of corresponding reserve assets.

(2) Each Issuer must honour user redemption requests in a timely, transparent and reliable manner, subject to the terms and conditions approved by the Regulatory Authority.

(3) Reserve accounts must be reconciled on a [daily] basis with internal recordkeeping systems capable of real-time balance tracking.

(4) Issuers must ensure that redemption of Stablecoins into fiat currency is available within one business day (T+1), without undue delay or material discount.

Explanatory Note:

This section ensures Stablecoin Issuers continuously match circulating tokens with corresponding reserves and honour redemption requests reliably and transparently. It reinforces operational discipline, protects user confidence and empowers the regulator to set standards for reconciliation, reporting and timely redemption procedures.

21. Risk-Based Reserve Management

(1) Issuers must adopt and implement a written reserve management policy that includes—

(a) procedures for mitigating liquidity risks, including stress-testing under adverse scenarios;

(b) controls for market risk, including mark-to-market valuation of assets;

(c) systems for managing operational risk, including cybersecurity protocols; and

(d) systems for assessing, monitoring and managing Stablecoin Activities performed by third parties.

(2) The policy referred to in subsection (1) must be reviewed and updated annually, at a minimum.

Explanatory Note:

This section requires Stablecoin Issuers to adopt written policies addressing liquidity, market and operational risk – reflecting a forward-looking, risk-based approach to reserve management. It extends oversight to third-party service providers and mandates annual reviews to ensure ongoing alignment with systemic and technological changes. The regime supports global prudential standards and bolsters user fund protection.

22. Phased Reserve Model for Stablecoin Issuance

(1) Issuers must adhere to the following three-phase prudential reserve model or as otherwise prescribed by the Regulatory Authority—

(a) Phase 1: full (1:1) reserve backing with no interest-bearing instruments permitted in the reserve;

(b) Phase 2: full (1:1) reserve backing permitted with interest-bearing reserve instruments approved by the Regulatory Authority;

(c) Phase 3: partial reserve backing with mandatory enhanced prudential oversight, systemic risk buffers and liquidity requirements permitted with the approval of the Regulatory Authority.

(2) Progression between phases is subject to Regulatory Authority approval based on systemic risk assessments, market maturity and Issuer compliance history.

Explanatory Note:

This phased reserve framework balances regulatory certainty with innovation enablement, progressing through three defined stages—

(a) Phase 1 mandates full (1:1) reserve backing with no interest-bearing instruments, ensuring strong customer protection and financial stability during early adoption.

(b) Phase 2 introduces capital optimisation through risk-managed reserve strategies.

(c) Phase 3 allows fractional reserves only where supported by adequate market, legal and prudential safeguards – ensuring alignment with global prudential standards.

Phase 3 access is strictly limited to Issuers and requires prior approval from the Regulatory Authority. Progression between phases is subject to regulatory evaluation based on systemic risk, market maturity and the Issuer's compliance history.

By deferring the authorisation of fractional reserve practices to national regulators, the framework accommodates the diverse legal, supervisory and financial stability environments across countries.

23. Tiered Reserve Requirements

(1) Issuers must be subject to the minimum prudential, capital buffer and reserve requirements set out in Exhibit A.

(2) Tier 1 Issuers must—

(a) hold 100 per cent reserve backing in High-Quality Liquid Assets;

(b) have a minimum of specified reserve assets or [US$10 million] (or currency equivalents) as a capital buffer;

(c) segregate user accounts;

(d) submit reserve attestation reports to the Regulatory Authority monthly;

(e) conduct biannual financial audits; and

(f) make real time (24/7) reserve holdings disclosures that reflect current reserve composition, location and custodial arrangements publicly available in a format approved by the Regulatory Authority.

Explanatory Note:

Commonwealth member countries may mandate reserve thresholds based on their domestic economic context.

Real-time reserve reporting provides continuous transparency and trust in Tier 1 Stablecoins. This section enables immediate verification by users and regulators and enhances systemic oversight – critical for Stablecoins with the highest

adoption or systemic impact. There are a variety of safety and soundness factors, including the availability of an insurance fund in setting the appropriate minimum percentage of reserve assets.

Regular reserve reporting improves market transparency and allows for better monitoring of systemic risks by regulators and users alike.

(3) Tier 2 Issuers must—
  (a) hold 100 per cent reserve backing in High-Quality Liquid Assets;
  (b) have a minimum of specified reserve assets or [US$2 million] (or currency equivalents) as a capital buffer;
  (c) conduct biannual financial audits and risk management reporting.

(4) Tier 3 Issuers must—
  (a) hold a minimum [80 per cent] backing in High-Quality Liquid Assets with cash equivalent;
  (b) have [US$100,000] (or currency equivalents) minimum paid-up capital.

(5) Tier 0 Issuers—
  (a) have no reserve requirement but are subject to mandatory disclosures based on prudential requirements; and
  (b) must have redemption rights and restrictions approved by the Regulatory Authority.

24. Reserve Coverage Minimums

(1) Issuers must maintain reserve assets equal to the outstanding value of issued Stablecoins on at least a 1:1 basis.

(2) The Regulatory Authority may prescribe a minimum threshold in monetary terms in addition to percentage-based requirements.

(3) Where Stablecoins offer yield or involve complex risk structures, the Regulatory Authority may require—
  (a) reserve holdings in excess of 100 per cent; and/or
  (b) additional capital buffers and liquidity stress coverage.

Explanatory Note:

Reserve coverage minimums refer to the required ratio or amount of reserves a Stablecoin Issuer must hold relative to its outstanding liabilities (typically circulating Stablecoins). For example, a 100 per cent reserve coverage minimum means each Stablecoin must be backed 1:1 by eligible reserve assets. In some countries, especially those embracing risk-based regimes, higher coverage ratios might apply depending on the quality and volatility of the reserve assets. This section integrates global benchmarks such as the EU's MiCA and as prescribed under the Hong Kong Stablecoin Act, both of which require 1:1 reserves, while providing flexibility for minimum thresholds (e.g., US$1million–US$5 million) and percentage-based risk scaling (e.g. 100–130 per cent for high-risk models). The goal is to preserve redeemability and protect users without imposing disproportionate burdens on emerging Issuers.

25. Independent Audit Requirements

(1) Issuers must appoint an independent auditor, approved by the Regulatory Authority, to conduct quarterly audits verifying—

(a) the sufficiency and composition of reserve assets;

(b) adherence to liquidity and solvency requirements; and

(c) the effectiveness of risk management and reserve controls.

(2) Audit reports must be submitted to the Regulatory Authority within thirty (30) days of completion and made available for public inspection.

(3) Notwithstanding subsection (2), the Regulatory Authority may extend the period for submitting audit reports upon the request of an Issuer.

Explanatory Note:

Under this Model Law, all audits must be conducted by independent, licensed third-party auditors. This ensures objectivity and reduces the risk of conflicts of interest in the audit process, aligning with international best practices (e.g., IOSCO Audit Quality Framework).

26. Regulatory Reporting

(1) Each Issuer must prepare and submit such reports, returns and disclosures as may be required by the Regulatory Authority under this Act, the principal Act or any other applicable law.

(2) Issuers must submit to the Regulatory Authority, in the prescribed form and frequency—

(a) a breakdown of reserve asset composition by type, value, location and custodial institution;

(b) redemption performance and outstanding liabilities;

(c) results of liquidity and stress-testing exercises; and

(d) any material changes in risk management policy or governance structure.

Explanatory Note:

By this section, the Regulatory Authority expects Issuers to conduct stress-testing annually or when significant changes occur in their business, strategy or risk profile. Stress-testing should align with the nature, scale, complexity and risk profile of the Issuers' operations and include three scenarios—

(a) internal failure (idiosyncratic scenario);

(b) market-driven stress (systematic scenario); and

(c) combined stress (both internal and market-driven).

Stress tests should account for risks like credit or market losses on backing assets and sudden mass redemption demands that may require asset liquidation under unfavourable conditions. The tests should identify uncovered losses, liquidity shortfalls or capital inadequacies, and assess the duration and recovery path of stress events. Results should inform actionable contingency plans to address vulnerabilities.

(3) The Regulatory Authority may issue rules, guidelines, or directives specifying the scope of reporting obligations, including but not limited to—

(a) reserve composition and valuation;

(b) transactional volumes and redemption activity;

(c) risk exposure metrics and liquidity positions; and

(d) any material events or changes affecting the Stablecoin Activities of the Issuer.

Explanatory Note:

This section creates a broad and flexible reporting duty, empowering the Regulatory Authority to tailor requirements over time while maintaining legal clarity.

(4) Issuers must comply with all other international regulatory reporting obligations set out in the principal Act, this Act or any other Acts, as appropriate.

Explanatory Note:

This section affirms that Stablecoin Issuers remain subject to all applicable international regulatory reporting obligations, including those arising under the principal Act, this Act or any related legislation.

It ensures continuity and alignment with overarching financial supervisory frameworks, particularly in areas such as AML, CTF, cross-border prudential standards and financial integrity measures. The clause reinforces the principle that Stablecoin Activities must be integrated into the broader regulatory perimeter and are not exempt from international compliance norms.

27. Public Disclosure Obligations

(1) Each Issuer must make such public disclosures as are necessary to ensure transparency, promote market integrity and enable users to make informed decisions regarding Stablecoin Activities.

(2) In addition to section 2(1)(n) and section 11 of the principal Act, an Issuer must publish information at least monthly, on its publicly accessible website, including- of the principal Act, an Issuer must publish information at least monthly, on its publicly accessible website, including—

(a) valuations, custodianship arrangements, maturity profiles and location of reserve assets, ensuring interoperability with regulatory and public monitoring requirements;

(b) its Stablecoin redemption policies and liquidity framework, including—

(i) if redemptions are not guaranteed at par; and

(ii) conditions for redemptions (fees, processing times, minimum amounts;

(c) summaries of audit findings, including—

(i) auditor details (name, qualifications, etc.);

(ii) a statement by the Issuer's management that reserves adequately support Stablecoins in circulation;

(iii) examination scope and period covered;

(iv) detailed information on backing assets (types, amounts, valuation methods);

(v) custodial arrangements for safekeeping assets;

(vi) auditor findings and opinion on reserve adequacy;

(vii) risk disclosures (e.g., de-pegging, liquidity risks);

(viii) date of any statements or attestation reports;

(ix) signatures from the auditor and Issuer management;

(d) notice of any material operational, legal or governance changes, including an updated White Paper detailing—

(i) business description;

(ii) rights and obligations of Stablecoin holders;

(iii) risks affecting Stablecoin stability and Issuer obligations;

(e) its investment policy and backing assets, including types, Issuers and target credit ratings;

(f) information to clients on—

(i) Stablecoins in circulation;

(ii) composition and market value of backing assets;

(iii) data updated monthly or upon client request (not older than 30 days);

(g) Risk overview, including—

(i) business activities and associated risks;

(ii) risk management policies;

(iii) current and emerging risks.

(3) The information referred to in subsection (1) must be presented in a clear and comprehensible manner, in accordance with standards prescribed by the Regulatory Authority.

(4) Issuers must publish periodic reserve asset disclosures in a machine-readable format, which must detail asset composition, valuation methodologies, custodianship and maturity structure.

(5) Issuers must conduct and publicly disclose the results of periodic stress tests evaluating the adequacy, liquidity and resilience of reserve assets under simulated adverse market conditions in structured data formats and explanatory methodologies.

(6) All customers of Issuers must receive a regulatory-approved risk disclosure statement at onboarding and at regular intervals, summarising redemption rights, reserve composition, custodial risks and governance practices.

(7) The structure in Exhibit E may serve as a model for the White Paper and user disclosure obligations set out in this section.

Explanatory Note:

Market-making arrangements are essential for providing liquidity and stability to Stablecoins by facilitating continuous buy and sell orders, reducing price slippage.

The Regulatory Authority—

(i) requires Issuers to establish due diligence processes to assess market makers, ensuring risks are identified, managed, monitored and mitigated. Additionally, Issuers must have systems and processes to oversee, monitor and report risks promptly, enabling senior executives to take swift action and escalate issues when necessary;

(ii) uses a proportionality principle to assess VA businesses based on their risk profiles, which vary by nature, scale, complexity and inherent risks. VA businesses with higher risks must adopt more robust governance and risk management frameworks; and

(iii) evaluates compliance collectively, by the criteria in section 2(1)(n) of the principal Act and explained in the related commentary, to ensure the conduct of such businesses aligns with its prudential objectives.

(8) The Regulatory Authority may prescribe, by rule or directive, the scope, content, frequency and format of such disclosures.

28. Governance Disclosures

(1) An Issuer must disclose to the Regulatory Authority in the prescribed form and at the prescribed frequency—

(a) the governance framework for reserve management, including board-level responsibilities and delegated authorities;

(b) the composition and mandate of the risk and audit committees, including the frequency of meetings and the processes for reporting to the board; and

(c) the measures adopted to identify, manage and disclose conflicts of interest, including related-party transactions involving reserves.

Explanatory Note:

This section strengthens transparency and accountability in the management of reserves by requiring Issuers to maintain and report on robust governance structures. It mandates disclosure of board oversight mechanisms, committee functions and conflict-of-interest controls.

The inclusion of a prescribed form and frequency ensures the Regulatory Authority receives consistent, comparable and timely information necessary for supervisory assessment and enforcement. This section aligns with international standards on sound governance and reserve integrity, as recommended by FSB and IOSCO for Stablecoin arrangements.

(2) In the case of a Stablecoin governed by a DAO, an Issuer must—

(a) publish on a public, accessible medium—

(i) governance rules and voting mechanisms;

(ii) upgrade and change management procedures;

(iii) allocation and use of treasury funds;

(b) Implement and disclose—

(i) multi-party authorisation (M-of-N) for key protocol functions;

(ii) independent third-party review of smart contracts;

(iii) identification of key signatories and voting power distribution.

(3) Where the DAO's governance affects the stability, security or redemption of the Stablecoin, such governance structure shall be subject to oversight and enforcement actions by the Regulatory Authority.

Explanatory Note:

This section introduces robust governance disclosure and control mechanisms for DAOs. Decentralised governance for Stablecoins enhances transparency, stability and trust by distributing decision-making authority. It reduces centralised risks, ensures auditability of reserves and allows community-driven adjustments to maintain financial integrity. Regulatory frameworks increasingly recognise decentralised models for their ability to provide secure, adaptable compliance mechanisms.

Governance requirements for algorithmic stablecoins are evolving rapidly, especially in light of past failures. While there is no universal standard yet, several key themes are emerging across jurisdictions and policy proposals.

(4) The Regulatory Authority may prescribe additional requirements in relation to the form and timing of such disclosures as it considers appropriate.

Explanatory Note:

This creates a broad but flexible foundation, allowing the Regulatory Authority to adapt disclosure requirements to evolving market risks and technological practices.

(5) Where failure to establish adequate internal systems, governance, training or controls materially contributes to breaches under this Act, executive officers, board members or controlling persons may be held personally liable in accordance with applicable law, regardless of whether direct intent or gross negligence is proven.

Explanatory Note:

This section aligns with accountability regimes under Basel III, and ISO 37301 on compliance management.

Part V
Prevention of Money Laundering and Terrorism Financing by Issuers

29. AML/CFT Compliance Requirements

(1) Issuers must comply with all applicable AML/CFT obligations imposed under Part IV in the principal Act and on [*insert name of Commonwealth member country*], the provisions of which are incorporated by reference in this Act.

(2) Issuers must conduct customer due diligence (identification and verification) at onboarding and appropriate monitoring of transactions, in accordance with international AML/CFT standards and subject to applicable data protection laws.

Explanatory Note:

Part V ensures the legal framework aligns with AML/CFT standards applicable to VASPs and VAs under the principal Act, including FATF Recommendation 15. It incorporates obligations to implement preventive measures, transaction monitoring, on-chain analytics and the Recommendation 16 Travel Rule to address the misuse of Stablecoins for illicit purposes. VASP must comply with national data protection laws, therefore the data protection laws of a Commonwealth member country, especially governing consent and cross-border data transfers, will be crucial in this regard.

The risk management provisions extend to Smart Contract vulnerabilities, cybersecurity threats and systemic risk scenarios. Risk-based obligations help balance innovation and regulation, allowing resource-efficient compliance for smaller entities while maintaining high standards for systemically important ones.

Key Concepts:

- FATF R.16 Travel Rule: a requirement for VASPs to share originator and beneficiary information during VA transfers.
- Enhanced Due Diligence: additional checks for high-risk transactions or clients.

Standard-Setter References:

- FATF R.15 and R.16 – specific to VAs and wire transfers
- Egmont Group – best practices for VASP supervision
- Principal Act – Part IV on AML/CFT compliance for VASPs

Part VI
Customer Protection

30. Rights and Protections for Stablecoin Users

(1) Each Issuer must conduct Stablecoin Activities in a manner that ensures the fair, transparent and prudent treatment of customers, and must implement appropriate measures to safeguard customer rights, interests and funds.

(2) Issuers must provide clear, accurate and fair disclosures to customers as prescribed by Part V of the principal Act, including—

(a) Stablecoin risks, including potential de-pegging, insolvency and liquidity constraints;

(b) redemption rights, specifying the process, fees and timeframes for converting Stablecoins back to fiat;

(c) terms of use, including dispute resolution mechanisms for users;

(d) reserve composition and the safeguards in place to protect customer funds;

(e) contribution to public financial education initiatives on digital asset risks, to be co-ordinated by the Regulatory Authority annually; and

(f) any other disclosure that the Regulatory Authority may consider necessary.

(3) Users must have access to—

(a) fair and transparent fees with no hidden charges;

(b) timely and accessible customer support for transaction-related issues; and

(c) a dispute resolution process in case of misconduct by Issuers.

Explanatory Note:

This section safeguards the interests of Stablecoin users by requiring Issuers to provide clear, fair and timely disclosures and services. These rights reflect established principles in financial consumer protection and ensure users can make informed decisions, access their funds under predictable terms, and seek redress when needed—

(a) Subsection (1) mandates transparency around key risk factors, redemption mechanics, usage terms and reserve practices – core areas where user confidence may be affected.

(b) Subsection (2) complements this by guaranteeing practical access to basic protections, such as transparent fees, responsive customer service and effective dispute resolution channels.

The provision supports broader regulatory goals of market integrity, user trust and financial inclusion, particularly as Stablecoins become more embedded in everyday payments and cross-border finance.

The Regulatory Authority should consider including:

(a) a mandate for maximum redemption timelines (such as T+1 for fiat currency redemptions and T+3 for redemptions involving other assets) as set out in subsection 30(2)(b);

(b) a clarification of the funding formula and payout limits for the Compensation Fund under subsections 32(1) and (2) (for example a 0.1 per cent annual contribution, with a maximum payout of US$10,000 per user);

(c) a prohibition on redemption gates such that Issuers may not suspend redemptions without obtaining prior approval from the Regulatory Authority as referenced in subsection 30(2)(b).

31. Fraud Prevention and Redress Mechanisms

(1) A licensed Stablecoin Issuer must implement and maintain effective systems, controls and procedures to detect, prevent and respond to fraudulent or abusive conduct in connection with Stablecoin Activities.

(2) Issuers must implement fraud detection mechanisms, including—
   (a) transaction monitoring to detect abnormal or suspicious patterns;
   (b) on-chain fraud detection tools to track illicit activities;
   (c) real-time alerts for high-risk transactions, such as large withdrawals or cross-border movements;
   (d) clear processes established and publicised for lodging complaints or claims related to fraud or unauthorised transactions; and
   (e) timely investigation, resolution and redress in accordance with standards prescribed by the Regulatory Authority.

Explanatory Note:

This section requires Stablecoin Issuers to implement systems to detect and prevent fraud, and to protect users against scams and unauthorised activity. It also mandates accessible redress processes for affected users, ensuring timely investigation and resolution. These obligations enhance consumer protection and operational integrity in line with global best practices.

32. Customer Redress Mechanisms

(1) The Regulatory Authority may establish or designate a Compensation Fund to provide redress to eligible users who suffer financial loss arising from fraud, mismanagement or insolvency.

(2) Contributions to the Fund may be required from licensed Stablecoin Issuers, based on criteria prescribed by the Regulatory Authority, including—
   (a) volume of issued Stablecoins;
   (b) level of user assets held; and
   (c) systemic risk designation or compliance history.

(3) Customers must have the right to file complaints with the Regulatory Authority, which must investigate cases in a timely manner.

(4) Stablecoin recovery and resolution procedures must be available in cases of unauthorised transactions or system failures.

Explanatory Note:

This section introduces more explicit customer remedies than the principal Act, with mandatory disclosures and redress that reflect lessons from prior market

failures. Redress mechanisms for Stablecoins differ from traditional finance in several key ways owing to the decentralised and digital nature of Stablecoins.

Unlike regulated Financial Institutions, Stablecoins often operate in a regulatory grey area, requiring custom dispute resolution. Instead of centralised oversight, Stablecoins may use decentralised governance or Smart Contracts for redress. Their instant transactions demand rapid dispute resolution, unlike the lengthy legal procedures in traditional finance. Global usage adds jurisdictional complexity, making enforcement difficult. However, Stablecoins benefit from transparent blockchain tracking, enabling automated resolution, whereas traditional finance relies on institutional oversight.

Key Concepts:

- Compensation Fund: a fund designed to reimburse customers in the event of Issuer insolvency or fraud.
- De-pegging Risk: the risk that a Stablecoin will deviate from its reference value.

Standard-Setter References:

- IOSCO – Stablecoin Public Consultation Reports on User Protections (2021–2023)
- FSB: Customer protection in cross-border Stablecoin arrangements

Part VII
Supervision and Enforcement

33. Enforcement Actions and Sanctions

(1) The supervision and enforcement powers of the Regulatory Authority as set out in Part VI of the principal Act are incorporated by reference in this Act.

(2) To the extent of inconsistency, this Act prevails over the principal Act.

34. Offences Relating to Stablecoin Activities

(1) A person commits an offence if they engage in any Stablecoin Activity in contravention of this Act; the principal Act; or any rule, directive or condition issued by the Regulatory Authority under this Act.

(2) It is an offence for any Person to knowingly engage in a Stablecoin Activity in contravention of this Act, including but not limited to—

(a) issuing or facilitating the issuance of Stablecoins without the appropriate licence;

(b) misrepresenting the value, redemption guarantee or reserve backing of a Stablecoin;

(c) wilfully failing to maintain reserves as required under Part IV;

(d) concealing, falsifying or materially misreporting financial, audit or reserve information;

(e) using Stablecoin platforms for the purpose of fraud, market manipulation, money laundering, terrorist financing or proliferation financing;

(f) operating a Stablecoin system in a manner that knowingly causes material risk to financial stability or systemic disruption.

(3) In determining the nature and extent of sanctions, the Regulatory Authority will consider—

(a) the scale and impact of the offence on users, markets and the financial system;

(b) whether the breach was deliberate, reckless or due to gross negligence;

(c) the steps taken by the offender to remedy the breach;

(d) whether the offender self-reported or co-operated with regulatory investigations;

(e) the offender's history of compliance and the presence of aggravating or mitigating circumstances.

(4) Sanctions under this section must be interpreted in a manner that reflects the proportionality principle and the overarching objects of this Act and the principal Act – namely, to ensure financial stability, promote trust in Stablecoin systems and safeguard customers and investors.

Explanatory Note:

This section establishes regulatory offences to safeguard the integrity of Stablecoin markets and protect users from misconduct. It introduces penalties for actions such as unauthorised issuance, misrepresentation of reserve backing, wilful breach of disclosure obligations and use of Stablecoins for illicit purposes (e.g., fraud, money laundering, or terrorist financing).

By clearly defining offence categories and their consequences, this section deters malicious behaviour, reinforces regulatory compliance and enhances public confidence in digital financial instruments. It also supports the broader enforcement framework by enabling supervisory authorities to take proportionate action against individuals and entities that undermine financial stability or user trust.

The structure and scope of offences should reflect internationally recognised standards for financial integrity and digital asset oversight.

This section enables rapid intervention to protect user funds and preserve financial stability, modelled on the Federal Deposit Insurance Corporation and other resolution authority frameworks.

35. Sanctions by the Court upon Conviction

(1) A Person convicted of an offence under section 34(2) will, upon conviction by the Court, be liable to sanctions that may include—

(a) monetary fines proportionate to the scale of harm and culpability;

(b) restriction orders from holding executive or governance roles in Financial Institutions or any other entity;

(c) restitution orders requiring the return of misappropriated customer funds or reserves;

(d) custodial sentences in cases of egregious criminal misconduct, such as wilful fraud, systemic abuse or persistent disregard for regulatory orders;

(e) any additional penalty that the [relevant court] considers appropriate.

(2) In determining the appropriate sanction, the [relevant court] must consider—

(a) the nature and gravity of the offence;

(b) the degree of harm caused to users, markets or financial stability;

(c) whether the offender acted dishonestly, recklessly or negligently; and

(d) any prior offences or aggravating circumstances.

Explanatory Note:

This section draws inspiration from FATF enforcement principles, IOSCO guidance on market abuse and financial sector norms that prioritise deterrence, remediation and systemic stability.

This Part provides a non-prescriptive yet serious framework for addressing offences related to Stablecoin Activities. It empowers countries to respond proportionately, whether the misconduct involves misrepresentation, operational negligence or criminal behaviour.

Part VIII
Financial System Integration and Cross-Border Compatibility

36. Cross-Border Recognition and Equivalence

(1) The Regulatory Authority may recognise the regulatory and supervisory framework of a foreign country for Stablecoins as equivalent to the standards set out under this Act, provided that certain conditions are met, including—

(a) the foreign country demonstrates adherence to internationally accepted regulatory standards, including those promulgated by FATF, FSB, BIS and IOSCO.

(b) the regulatory regime ensures comparable levels of prudential, technological and customer protection safeguards.

(c) the foreign Regulatory Authority maintains effective supervisory co-operation and information sharing arrangements with the Regulatory Authority.

(2) Upon recognition of equivalence, Issuers licensed under that foreign regime may be granted a licence, exemption or other regulatory relief in [*insert name of Commonwealth member country*], subject to any conditions imposed by the Regulatory Authority.

(3) The Regulatory Authority must maintain a public list of countries to be regarded as equivalent for the purposes of this Act, including any restrictions or conditions associated with such recognition.

(4) The Regulatory Authority may withdraw or suspend the equivalence status of a Commonwealth member country where material changes occur in the legal, regulatory or supervisory regime of the foreign Commonwealth member country that compromise the basis for recognition.

Explanatory Note:

This section enables mutual recognition of Stablecoin regimes across countries, provided those regimes meet equivalent standards for prudential soundness, AML/CFT compliance, cybersecurity, and customer and investor protection. It aligns with FATF's recommendations on international co-operation and information exchange and promotes regulatory interoperability, reducing duplication and enabling smoother cross-border operations. The provision also reflects best practices from the EU's MiCA regime (Title VIII – Third-Country Equivalence) and the UK's approach to substituted compliance.

The Regulatory Authority must provide guidance on reciprocity and public consultation in relation to equivalence decisions under section 36. For example:

(a) Foreign recognition may require the applicant's home jurisdiction to grant equivalent access to domestic entities (reciprocity).

(b) A minimum thirty (30)-day public consultation period may precede recognition decisions (consultation).

37. Cross-Border Co-operation and Information-Sharing

(1) The Regulatory Authority must co-operate whether through information-sharing, joint investigations or supervisory co-ordination, with—

(a) foreign financial regulators to ensure international compliance and prevent regulatory arbitrage;

(b) domestic law enforcement agencies and Financial Intelligence Units to detect and prevent financial crimes;

(c) international standard-setting bodies (e.g., FATF, IMF, BIS) to align with global best practices.

(2) Information-sharing mechanisms must be established for—

(a) cross-border AML/CFT investigations involving Stablecoins;

(b) regulatory harmonisation to enable interoperability between countries;

(c) joint enforcement actions where entities operate across multiple countries.

Explanatory Note:

This section enables collaboration between domestic and foreign regulators to supervise, investigate and enforce Stablecoin laws across countries. It supports information exchange, joint investigations and alignment with international standards, helping prevent regulatory gaps and mitigate systemic risk in global Stablecoin markets.

38. Financial System Integration and Cross-border Compatibility

(1) A licensed Stablecoin Issuer must ensure its systems, processes and governance arrangements are designed to support interoperability with—

(a) domestic payment systems, Financial Institutions and regulatory frameworks; and

(b) foreign payment networks, Stablecoin regimes and supervisory authorities, where applicable.

(2) Stablecoins must be designed for seamless integration with Financial Institutions, central banks and VASPs.

(3) Issuers must ensure compliance with international financial messaging standards, including ISO 20022, to enable cross-border compatibility.

(4) Stablecoins must support cross-chain interoperability mechanisms such as atomic swaps, bridge protocols and inter-block communication standards.

(5) On-chain identity verification must be integrated to meet regulatory requirements without compromising decentralisation.

Explanatory Note:

This Part outlines the tools available to regulators to supervise, investigate and enforce compliance with this Act. It provides for proportionate sanctions based on severity – from technical non-compliance to systemic fraud – and introduces powers to revoke licences and freeze assets. It also includes cross-border co-operation provisions to recognise the global nature of Stablecoins and enable information-sharing and joint enforcement. These mechanisms help mitigate regulatory arbitrage and promote regional alignment across Commonwealth jurisdictions.

The Regulatory Authority will issue the requisite guidance relating to:

(a) compliance with ISO 20022, including messaging standards and operational integration for Stablecoin systems; and

(b) the application of conflict of law principles clarifying that, where multiple legal frameworks apply, the stricter rule will prevail.

For the purposes of clarification—

(a) Subsection 38(4) refers to Inter-Blockchain Communication (IBC) standards, which enable secure communication between independent blockchains. These standards define protocols for data exchange, asset transfers and interoperability across different blockchain ecosystems.

(b) Subsection 38(5) refers to Decentralised Identifiers (DIDs) applicable to Stablecoins. DIDs relate to self-sovereign identity systems that enhance security, transparency and compliance. They enable Stablecoin Users and Issuers to verify identities without relying on centralised authorities, thereby strengthening privacy and fraud prevention.

Part IX
Information and Communication Technology

39. Information and Communication Technology Operational Resilience

Issuers must establish and maintain secure, resilient, recoverable and scalable information and communication technology (ICT) systems within the Stablecoin Ecosystem that conform to international ICT standards.

Explanatory Note:

This requirement is designed to address broader aspects of ICT infrastructure and operational dependencies that extend beyond information security or cybersecurity concerns. While cybersecurity and data protection are critical components of Stablecoin Ecosystems, effective regulation must also encompass the full ICT environment – such as system architecture, network resilience, software lifecycle management, interoperability and scalability.

The term "blockchain" is deliberately omitted in this context to reflect the evolving technological landscape. Stablecoin Ecosystems may rely on multiple DLTs, permissioned and permissionless networks, or hybrid infrastructures that include application programming interfaces, cloud computing and centralised databases, in addition to blockchain-based components. Issuers may operate within complex digital environments where critical dependencies lie outside their direct control or outside the blockchain layer entirely.

By broadening the regulatory lens to include the entire ICT ecosystem, this section ensures regulatory oversight remains technologically neutral, future-proof and comprehensive. It also acknowledges that financial stability, operational resilience, and investor and customer protection depend on the reliability and governance of all supporting systems – not just those based on blockchain.

40. Access Control

(1) Issuers must implement and maintain robust access management controls to ensure the confidentiality, integrity and availability of all technical components within the Stablecoin Ecosystem.

(2) All privileged access to the Stablecoin Ecosystem must be monitored for suspicious activity and alerts generated to appropriate personnel.

(3) Issuers must ensure access to the Stablecoin Ecosystem is restricted to personnel's role-specific needs, granted only after authorisation, and revoked immediately upon role termination, with automated enforcement and biannual audits.

Explanatory Note:

This section requires Stablecoin Issuers to implement strong access controls to protect critical systems, user data and digital assets. It mandates measures like multi-factor authentication and key management, along with regular reviews. These safeguards enhance cybersecurity and align with global standards for operational resilience and accountability.

41. Multi-Party Authorisation Controls

(1) Subject to subsection (2), no individual Person, nor any automated system acting on behalf of a single Person, may have unilateral authority to execute, initiate or approve any act concerned with the control and management of a Stablecoin.

(2) An Issuer must ensure that any act involved in the issuance, redemption, transfer or other material control or management of a Stablecoin or its reserve assets is subject to joint authorisation by no less than two Persons duly approved and appointed.

(3) The Regulatory Authority may—

(a) require Tier 1 and Tier 2 Issuers to implement verifiable M-of-N threshold authorisation mechanisms, including multi-signature wallets or hardware-based approval protocols; or

(b) mandate or approve the use of M-of-N controls where critical functions (e.g., reserve access, systemic redemptions or protocol updates) are involved, particularly for Tier 1 or systemic Stablecoin Issuers.

(4) Where necessary, a qualified independent third party, such as a licensed custodian, external auditor or trusted execution environment provider, may be required to verify or co-sign such authorisations for added assurance.

Explanatory Note:

This section—

(a) supports reserve composition and investment risk (by ensuring control over asset movements);

(b) aligns with redemption and liquidity requirements;

(c) reinforces technology and cybersecurity requirements, especially around access controls and operational resilience, and

(d) complements section 12(2)(b), which imposes fiduciary duties on Issuers to act in the best interest of VA holders.

This section introduces a mandatory multi-party authorisation (M-of-N) requirement for Stablecoin Issuance and reserve-related functions. It ensures no individual, or system controlled by a single actor, can independently initiate or approve critical transactions, reducing key-man risk and operational vulnerabilities.

By requiring at least two duly authorised Persons to act jointly, the provision enhances the integrity, transparency and accountability of Stablecoin operations. For systemic or high-value Issuers, the Regulatory Authority may additionally require that an impartial third party – such as a licensed custodian, external assurance provider or Smart Contract oracle – participate in or verify transaction authorisations. This aligns with international best practices on operational risk and segregation of duties (e.g., BIS Principles for Financial Market Infrastructures, FATF Guidance on Virtual Assets).

42. Key Management

(1) A licensed Stablecoin Issuer must implement secure key management practices to protect cryptographic keys used in the issuance, redemption, custody or transfer of Stablecoins.

(2) Key material must be protected from unauthorised access while not in use.

(3) Stablecoin key material operations must be conducted in a secure, audited environment free from unauthorised surveillance or access.

(4) Equipment must be pre-checked for tampering, software and hardware updates, and other vulnerabilities, and physical and technical safeguards must include restricted access and environmental controls.

(5) Stablecoin key material must be backed up and stored in a separate location from primary key material operations and the key material backups must be protected from unauthorised access and use, and environmental impacts.

(6) All key material operations must be documented, maintained and made known to relevant parties.

Explanatory Note:

This section establishes a duty for Stablecoin Issuers to adopt secure key management practices to safeguard cryptographic keys essential to the creation, redemption, custody and transfer of Stablecoins. Since these keys control access to digital assets and critical systems, their compromise can lead to significant financial and operational risks.

43. Wallet Security

(1) Issuers must implement security controls for both custodial and non-custodial environments, including safeguards to prevent unauthorised access, protect private keys and ensure the operational integrity of wallet systems.

(2) Issuers must implement risk mitigation measures for both custodial and non-custodial wallets.

(3) Issuers must store the majority of Stablecoin reserves in secure, offline cryptographic storage systems isolated from internet-connected environments.

(4) Only operational amounts necessary for daily transactions may reside in internet-exposed systems, subject to strict access controls and real-time monitoring.

(5) Subject to section 41, all transactions affecting Stablecoin reserves or protocol governance must require authorisation from multiple authorised signers.

(6) The minimum required signer thresholds to conduct transactions affecting Stablecoin reserves or protocol governance must be determined through documented risk assessments.

Explanatory Note:

This section requires Stablecoin Issuers to implement strong security measures for both custodial and non-custodial wallets. It focuses on protecting private

keys, enabling secure user authentication and guarding against unauthorised access or asset loss. The framework promotes user trust and aligns with industry standards for digital asset custody and endpoint security.

This section also reflects international best practices for operational resilience, cybersecurity and custodial safeguards in the context of Stablecoin issuance and management. Issuers are required to adopt a layered security architecture that distinguishes between offline reserve storage and internet-facing operational environments. The intent is to minimise exposure to cyber threats while preserving transactional efficiency.

Key principles include:

(1) segregation of reserve environments to prevent unauthorised access and systemic breaches;

(2) multi-signature controls and threshold-based authorisations to strengthen procedural governance, prevent unilateral control and mitigate insider risks;

(3) dynamic signer configurations, guided by documented risk assessments, to allow the framework to scale based on transaction volume, asset complexity or protocol design.

These obligations align with global cybersecurity benchmarks (such as ISO/IEC 27001, NIST SP 800-53) and draw on prudential requirements set by entities such as the Basel Committee and Principles for Financial Market Infrastructures. Commonwealth jurisdictions may further tailor these provisions to support emerging technologies via regulatory sandboxes, ensuring proportionality without compromising systemic safety.

For the purposes of this section, a non-custodian or unhosted Stablecoin wallet is a type of digital wallet in which the user retains exclusive control of the private keys associated with their stablecoins. No third-party service (including exchanges, wallet operators or custodians) has access to the wallet's assets or the authority to manage the funds.

44. Smart Contract Security

(1) Smart Contracts governing Stablecoin issuance, redemption and transactions must adhere to stringent security protocols appropriate to their risk classification.

(2) Smart Contract Custom Software Code must be independently audited before deployment, and audit reports must be made publicly accessible to enhance transparency and accountability.

(3) Governance mechanisms must be established to oversee the review, upgrade or modification of Smart Contracts, including clear procedures for stakeholder approval and risk management.

(4) Smart Contract Custom Software Codes must be tested before deployment using methodologies proportionate to the risks posed by the design of the Stablecoin, the scale and the operational complexity, including, but not limited to, peer review, execution simulation and testing techniques aligned with internationally recognised software code testing frameworks.

Explanatory Note:

This section requires Stablecoin Issuers to ensure that Smart Contracts Custom Software Codes used in core functions are secure, auditable and fault-tolerant. It mandates formal verification, independent audits and incident protocols to mitigate risks and uphold safe automation. These measures align with global best practices for digital asset infrastructure.

In Section 44, Regulatory Authorities may consider requesting formal verification of Smart Contracts for Tier 1 and 2, such as "Mathematical proof of correctness for critical functions," and mandate bug bounty programs for systemic Issuers.

45. Secure Coding Practices

(1) A Stablecoin Issuer shall adopt and maintain secure software development and coding practices across all custom-built systems that support the issuance, governance, custody or transfer of Stablecoins.

(2) Issuers must apply secure coding techniques to minimise vulnerabilities in custom software.

(3) Secure coding practices shall be reviewed periodically by the Issuer, and updated as necessary, having regard to industry-recognised standards.

Explanatory Note:

This section promotes secure software development by requiring Stablecoin Issuers to adopt standards such as code reviews, vulnerability testing and secure development lifecycles. It aims to reduce risks tied to software flaws, enhancing user protection and system resilience through alignment with industry-recognised frameworks.

46. Oracle Security

(1) Subject to subsection (2), Issuers must ensure all oracles and external data sources integral to Stablecoin Issuance, redemption or stability mechanisms are secure, reliable and resilient to manipulation.

(2) Issuers must implement redundancy measures, third-party audits of oracle systems and real-time monitoring for anomalies to ensure compliance with the requirement in subsection (1).

Explanatory Note:

This section addresses the reliability and resilience of oracles used in Stablecoin systems by requiring strong governance, authentication and integrity verification. It mitigates risks from data manipulation or failure and supports regulatory oversight to ensure trust in externally sourced, automated data flows.

47. Human Resource Security

(1) Issuers must ensure all personnel who can affect the confidentiality, integrity and availability of the Stablecoin Ecosystem are aware of their roles and responsibilities and formally acknowledge them in writing.

(2) Issuers must ensure each personnel under their control with access to the Stablecoin Ecosystem undergoes pre-employment and periodic background criminal and identification checks conducted by approved third-party providers.

(3) Such checks must assess integrity; criminal history; and potential, contingent or real conflicts of interest, with exemptions permitted only where prohibited by applicable local law.

(4) Where local laws restrict background, criminal and identification checks, Issuers must implement compensating controls to mitigate risks from unvetted personnel.

Explanatory Note:

This section establishes minimum human resource security standards for Issuers, particularly where staff have access to systems, data or processes critical to the confidentiality, integrity and availability of the Stablecoin Ecosystem.

The requirement for pre-employment and ongoing background checks ensures that personnel entrusted with sensitive tasks are vetted for integrity, criminal history and identification verification. These checks are to be conducted by independent, qualified third parties to ensure objectivity, consistency and high standards of due diligence. This approach is critical because past reliance on internal human resources processes – without independent oversight – has led to weak or incomplete vetting, exposing systems to insider threats or compliance failures.

"Third parties" in this context refers to any entity appropriately licensed, accredited or otherwise qualified under law or regulatory guidance to conduct such checks. This flexible definition allows countries to adopt context-appropriate standards while maintaining robust vetting practices.

Furthermore, the provision recognises that some countries may impose legal limitations on conducting certain types of background screening. In such cases, Issuers are required to implement compensating controls – such as enhanced monitoring, restricted access, segregation of duties or mandatory probation periods – to manage risks associated with unvetted or partially vetted personnel. This framework reflects best practices from global ICT and cybersecurity standards (e.g., ISO/IEC 27001, NIST SP 800-53), which underscore the importance of personnel security in mitigating operational, governance and cybersecurity risks in financial and VA ecosystems.

48. Technology and Cybersecurity Requirements

(1) Issuers must ensure only operational amounts necessary for daily transactions reside in internet-exposed systems, which must be subject to strict access controls, multi-factor authentication and real-time monitoring to detect and prevent unauthorised access or cyber intrusion.

(2) Issuers must conduct cybersecurity assessments in accordance with templates prescribed by the Regulatory Authority.

(3) The Regulatory Authority may prescribe minimum technology and cybersecurity and assessment requirements as set out in Exhibits C and D.

Explanatory Note:

This section reinforces cybersecurity and operational risk controls by limiting exposure of liquidity to internet-facing systems. It mandates encryption, authentication and monitoring for secure transactions and aligns with international best practices. It also authorises prescribed templates under section 48 and supports supervisory guidance under section 59, promoting resilience and regulatory compliance, especially for systemic Issuers. An illustrative template referred to in subsection (3) is provided in Exhibit D.

This section also reflects best practice from global standard-setters, including FATF, IOSCO and FSB, which emphasise segregation of reserves, use of cold storage for systemic holdings and continuous threat monitoring. It also supports compliance with operational resilience and prudential standards applicable to Tier 1 and Tier 2 Issuers.

49. Monitoring and Incident Response

(1) A Stablecoin Issuer must implement continuous monitoring systems and incident response protocols to identify, assess and respond to operational disruptions, cybersecurity threats or other incidents affecting Stablecoin Activities.

(2) Issuers must implement real-time monitoring of relevant blockchain activity to detect anomalies affecting Stablecoin reserves or protocol governance.

(3) Automated alerts must trigger predefined response protocols, with incidents escalated to qualified personnel for investigation and remediation.

(4) Issuers must establish an incident response management plan to address security breaches and operational system failures.

(5) Incident response teams must be trained and conduct regular drills to test response effectiveness and cover threat scenarios identified in the ICT risk assessment.

(6) Issuers must subscribe to and integrate intelligence feeds from qualified third-party providers to monitor current and emerging threats that could impact the security of the Stablecoin Ecosystem.

Explanatory Note:

In this section, monitoring and incident response for Stablecoins ensure security, compliance and financial stability—

(a) Monitoring involves real-time surveillance of transactions to detect fraud, reserve asset tracking to verify backing, on-chain compliance tools for AML/know-your-customer and Smart Contract audits for security vulnerabilities.

(b) Incident response includes rapid breach detection, dispute resolution mechanisms, regulatory reporting of security issues and cyber resilience plans to handle cyberattacks.

(7) Issuers must implement systems to continuously identify, assess, treat and monitor cybersecurity threats to the issuing platform, including the Stablecoin Smart Contract infrastructure, reserve management systems and user interfaces.

(8) Minimum systems required under subsection (4) must include—
(a) event-based logging;

(b) Smart Contract change detection; and

(c) anomaly alerting mechanisms.

(9) The level of monitoring must be commensurate with the scale, complexity and risk profile of the Issuer, and must escalate proportionally with tiered classification under section 13.

(10) The Regulatory Authority may issue rules, guidance or technical standards prescribing the minimum acceptable controls for each tier under this subsection.

Explanatory Note:

This section reinforces the operational resilience obligations of Issuers, ensuring continuous threat assessment and mitigation across critical systems. It complements section 47(1)–(4) and aligns with international standards, including guidance issued by FATF (Recommendation 15) and BIS (2023 Report on Crypto Asset Resilience) and the IOSCO–FSB Joint Recommendations on Stablecoins.

Minimum baseline expectations include event-based logging (recording system activity for traceability), Smart Contract change detection (to flag unauthorised or malicious modifications) and anomaly alerting (identifying behavioural deviations suggestive of cyber compromise).

Such controls are achievable using open-source tools or commercial solutions and do not require enterprise-grade Security Operation Centre (SOC) deployments. These expectations apply to all tiers under the Tiered Licensing Framework and intersect with reserve protection obligations, disclosure of governance and operational risks, and cybersecurity compliance attestations.

Scaling with risk and impact: As entities scale or transition to higher tiers under section 14, their obligations will intensify. This may include—

(a) integration into real-time Security Information and Event Management (SIEM) dashboards;

(b) use of AI-based anomaly detection tools;

(c) periodic third-party audits or certifications; and

(d) integration into enterprise risk governance frameworks.

Entities meeting higher standards may benefit from faster approvals, reduced reporting burdens or reputational advantages.

In section 49(8)(b), Smart Contract change detection refers to detecting redeployments, proxy contract changes or on-chain code discrepancies, since Smart Contracts are generally immutable.

50. Governance and Risk Management

(1) Issuers must establish and maintain an ICT governance framework ensuring a documented ICT strategy with policies, standards and procedures that enforce multi-layered ICT controls, continuous monitoring and improvement, and that align with international ICT standards.

Explanatory Note:

This section broadens regulatory scope by referencing "international ICT standards" to encompass infrastructure, data governance and cybersecurity. It enables recognition of global frameworks like ISO/IEC 27001, the CryptoCurrency Security Standard (CCSS) and/or SOC 2, ensuring high standards for operational resilience while allowing regulatory flexibility to accommodate evolving technologies and equivalent certifications.

(2) The minimum governance and risk management checklist requirements set out in Exhibit B apply to all tiered Issuers.

(3) Issuers must implement a comprehensive ICT risk management framework.

(4) Issuers must establish and maintain robust business continuity, disaster recovery and resolution policies designed to ensure the uninterrupted provision of critical services in the event of cyberattacks, liquidity shortfalls or critical system failures, which must—

(a) be tested at least annually and include clearly defined recovery time objectives;

(b) provide for the use of redundant systems and infrastructure to minimise disruption;

(c) include contingency funding plans and liquidity management frameworks to address financial shocks; and

(d) align with internationally recognised standards for operational resilience and user fund protection.

Explanatory Note:

This section imposes a proactive obligation on Issuers to plan for extreme but plausible disruptions, ensuring operational continuity and financial stability in adverse scenarios. Key elements of the accompanying policies include—

(a) risk scenario planning: anticipating cyberattacks, liquidity stress and infrastructure failures, with proportionate recovery frameworks;

(b) documented recovery and contingency plans: establishing formal recovery protocols and contingency funding to maintain solvency;

(c) orderly wind-down procedures: ensuring structured cessation of operations if recovery efforts fail, minimising user impact;

(d) purpose and outcomes: identifying and mitigating financial risks, ensuring predictability in business models and maintaining adequate financial and technical resources.

This section also aligns with international standards such as those from FSB, IOSCO and FATF, and reflects a maturing approach to operational resilience in the VA sectors.

Regulatory Authorities may clarify that existing issuers must freeze user growth until licensed, require public notice of transitional status (e.g., website disclosure banners) and add exit conditions for sandbox (Tier 0) participants (e.g., must migrate to Tier 3 within twelve to twenty-four (12–24) months).

(5) Issuers must conduct appropriate due diligence and implement ongoing monitoring and periodic review of all third-party service providers capable of affecting the integrity, security, operational resilience or continuity of Stablecoin Issuance or related activities.

Explanatory Note:

Third-party service providers are often overlooked when an entity is defining its information security management system (ISMS), trusting that the service provider will ensure its own operational security is up to the level of or higher than the entity's.

A failure or compromise at a third-party service provider could impact the security of the Issuer's operational activities, thereby jeopardising market confidence and broader financial stability of the Stablecoin. The requirement ensures each Issuer, prior to engagement and on a continuing basis, undertakes proportionate due diligence enquiries into every service provider that may affect the integrity, security, operational resilience or continuity of the Stablecoin. Furthermore, the Issuer should continuously monitor the security posture of the third-party service provider to ensure its security posture remains at the Issuer's required level.

Security controls to consider when conducting due diligence and continuous monitoring should include information security posture, updates on remediation activities of the service providers' security controls, a risk register, business continuity and disaster recovery capabilities, a governance structure and the service providers' own continuous monitoring and improvement processes for their ISMS.

(6) Ongoing audits and assessments must be conducted to ensure compliance with international ICT standards.

Explanatory Note:

This Part integrates ICT governance and operational activity into the legal framework, requiring secure, resilient, recoverable and scalable ICT systems used within the Stablecoin Ecosystem. Of particular focus is the security of the people, processes and technology components that make up the Stablecoin Ecosystem. This Part ensures effective information security controls are established, maintained, monitored and improved upon for not only the technical components of the Stablecoin Ecosystem but also the people and processes within the Stablecoin Ecosystem.

Key Concepts:

CCSS Glossary definition: "The parameters used to derive or represent cryptographic keys, includes the raw components such as seed phrases, private keys, public keys, or key shares that are fundamental to encryption, decryption, signing, or verifying digital information".

Standard-Setter References:

- CCSS – key management standard for VAs
- ISO/IEC 27001 – global baseline for ISMS
- Payment Card Industry (PCI) Data Security Standard (DSS) version 4.0.1 – global information security standard for systems that transmit, process or store credit card data

This Model Law does not require an Issuer to hold certification to internationally recognised information security standards or to obtain third-party assurance reports. Nevertheless, Issuers are encouraged to—

(a) seek certification to ISO/IEC 27001, the CSS, and/or

(b) commission independent assurance engagements (e.g., SOC 2 Type I/II reports)

Certifications can provide additional assurance to stakeholders regarding the adequacy and effectiveness of the Issuer's ICT-security controls.

This Model Law acknowledges that new international information security standards for blockchain and DLT systems will be developed and adopted in the future and could be better suited than the standards mentioned in this Model Law.

(7) For the purposes of section 50(4) and section 50(6), the cybersecurity controls listed in Exhibit C are considered baseline tiered requirements and may be supplemented by the Regulatory Authority under section 54.

Explanatory Note:

Although section 50 integrates these as baseline controls, explicitly cross-referencing Exhibit C affirms legal enforceability.

Part X
Transitional Provisions and Final Provisions

51. Licensing Requirements

(1) Existing Issuers prior to the commencement of this Act must—

(a) apply for a licence under this Act within [six (6) months] from the commencement date; and

(b) cease any activity not permitted under this Act until such licence is granted or denied.

(2) Existing Issuers must, within a transitional period to be prescribed by the Regulatory Authority—

(a) comply with minimum reserve requirements, AML/CFT obligations, cybersecurity standards and customer protection measures set out in this Act;

(b) submit a Regulatory Impact Assessment Report demonstrating their current operations, risk exposures, compliance strategies and mitigation plans.

Explanatory Note:

This section supports measured implementation, a principle also embedded in the principal Act, ensuring legal continuity and stakeholder readiness. Commonwealth member countries may customise timelines to suit their domestic context.

Key Concepts:

- Regulatory Impact Assessment: an analysis that evaluates the effect of new regulation on stakeholders and the economy.

Standard-Setter References:

- OECD – guidelines for Regulatory Impact Assessment
- FATF – encourages regular review and phased compliance for VA frameworks

52. Temporary Relief and Phased Compliance

The Regulatory Authority may, on a case-by-case basis, grant transitional relief or staggered compliance schedules to existing Issuers, provided that—

(a) a credible and time-bound compliance roadmap is presented and approved;

(b) no material risk to financial stability, market integrity, investors or customers arises from the temporary exemption.

53. Appeals

(1) A Person may appeal to the [Appellate Body] against a decision of the Regulatory Authority to take enforcement action.

(2) The appeal must be made within [X] days of the decision of the Regulatory Authority.

(3) In determining an appeal, the [Appellate Body] may—

(a) confirm, vary or revoke the decision of the Regulatory Authority; and

(b) make further orders as it considers appropriate.

Explanatory Note:

Commonwealth member countries may determine the appellate process and timelines based on their market readiness and applicable judicial systems.

54. Customer and Market Communication

Issuers transitioning to compliance must issue timely and transparent notifications to affected customers, counterparties and the public, as directed by the Regulatory Authority.

Explanatory Note:

This section ensures that Stablecoin Issuers communicate transparently and accurately with users and the market. It mandates clear disclosures on product features and risks, requires timely updates on material changes and supports global standards for market conduct and consumer protection, thereby fostering trust and informed decision-making.

55. Amendment and Review

(1) The Regulatory Authority must conduct a comprehensive review of this Act [every three (3) years], or at such intervals as may be necessary to—

(a) evaluate the efficacy and proportionality of the regulatory framework;

(b) identify emerging risks and supervisory blind spots;

(c) integrate new developments in financial technology, decentralised finance and VAs;

(d) ensure alignment with evolving international standards and commitments set by bodies such as FATF, IOSCO, FSB, IMF and BIS.

Explanatory Note:

In this section, Decentralised Finance (DeFi) refers to a financial system built on blockchain technology that eliminates traditional intermediaries like banks and brokers. Instead, it relies on Smart Contracts and decentralised applications (dApps) to facilitate transactions directly between users.

Key Features of DeFi:

(a) Peer-to-Peer transactions: users can lend, borrow, trade, and earn interest without needing a centralised authority.

(b) Transparency: all transactions are recorded on a public blockchain, ensuring openness.

(c) Accessibility: anyone with an internet connection can participate, without needing approval from Financial Institutions;

(d) Automation: Smart Contracts execute transactions automatically based on predefined conditions.

Common DeFi Applications:

(a) Lending and borrowing: platforms like Aave and Compound allow users to earn interest or take out loans.

(b) Decentralised Exchanges: services like Uniswap enable users to trade cryptocurrencies without intermediaries.

(c) Stablecoins and yield farming: users can earn passive income by providing liquidity to DeFi protocols.

While DeFi offers financial freedom and innovation, it also comes with risks such as hacks, Smart Contract vulnerabilities and regulatory uncertainty.

(2) Public consultation is required in amendment cycles (thirty to sixty (30–60) days) and requiring review to reflect latest international standards.

(3) Amendments to this Act or the issuance of supplementary instruments must, to the extent practicable, involve public consultation and engagement with industry participants, customer and investor protection bodies, and relevant domestic and international regulatory stakeholders.

56. Interpretation and Hierarchy

(1) This Act must be read in conjunction with—

(a) the principal Act, to the extent that Stablecoin Activities intersect with the provision of VA services;

(b) applicable national financial services, securities, AML/CFT, insolvency, and investor and customer protection laws.

(2) In the event of conflict, the following must prevail—

(a) the objectives of financial stability, market integrity, customer and investor protection, and responsible innovation;

(b) the international obligations of [*insert name of Commonwealth member country*], including commitments under mutual evaluations or treaty frameworks.

57. Legal Continuity

(1) All licenses, permits or approvals granted under previous regulatory frameworks relating to Stablecoin Activities must remain valid for the duration of the transitional period, subject to revalidation under this Act and as determined by the Regulatory Authority.

(2) Such authorisations will be subject to revalidation, modification or revocation under this Act, based on criteria established by the Regulatory Authority and any guidance it may issue.

(3) Issuers operating under pre-existing approvals must apply for recognition or renewal within a prescribed timeframe set out in transitional regulations, failing which such approvals may lapse upon expiry of the transitional period.

58. Regulatory Guidelines

(1) The Regulatory Authority may issue such supplementary rules, guidelines, regulatory circulars, protocols, codes of practice or binding directions as may be necessary to give full effect to the provisions of this Act or to provide for its proper administration, supervision and enforcement.

(2) Without limiting the generality of subsection (1), such rules, guidelines, protocols, codes or directions may include provisions relating to—

(a) prudential and conduct standards for yield-bearing Stablecoins, including but not limited to licensing requirements, risk disclosures, asset segregation, product suitability, liquidity risk management and capital adequacy frameworks;

(b) governance, audit and reserve transparency requirements for algorithmic and DAO-issued Stablecoins, including stress-testing, failure scenarios, reserve composition disclosures and automated stabilisation mechanisms;

(c) tiered classification criteria and associated obligations for Stablecoin Issuers, based on activity scale, user base, financial exposure or systemic importance;

(d) cross-border issuance, usage and redemption of Stablecoins, including interoperability protocols, regulatory passporting and compliance with foreign country requirements;

(e) technology, information-security and cyber-resilience requirements, covering governance and baseline controls, secure consensus and secure software code practices, continuous threat monitoring, incident response and business continuity planning, as well as equivalent standards for critical third-party service providers;

(f) AML, CTF and counter-proliferation financing obligations for Stablecoin Activities, consistent with international standards;

(g) complaint handling, dispute resolution and customer protection mechanisms applicable to both issuers and service providers;

(h) memoranda of understanding required for co-ordination between the central bank, securities regulator, data protection authority and financial intelligence unit; and

(i) any matter necessary or incidental to the exercise of the functions of the Regulatory Authority under this Act.

Explanatory Note:

This section empowers the Regulatory Authority with broad and flexible rulemaking authority to ensure the dynamic and risk-sensitive supervision of Stablecoins, particularly in high-risk areas such as yield-bearing and algorithmic issuance models.

Given their complexity and potential systemic implications, this section allows for responsive regulatory development aligned with evolving international standards (including FATF, IOSCO, FSB and IMF guidance). It also provides legal certainty for cross-border operations and technology-related obligations under the Act.

This Part ensures a smooth transition for existing Stablecoin Issuers and service providers through a structured compliance window and regulatory oversight. It introduces a review cycle every three (3) years to maintain legal relevance in a fast-evolving space.

59. Regulations

For the purposes of this Act, the [Minister/Regulatory Authority] may make such [delegated legislation] as [she]/[he]/[it] thinks fit.

Explanatory Note:

Commonwealth member countries may consider inserting other provisions, such as savings provisions as well as consequential amendments, as necessary.

60. Commencement

This Act will come into force on the day on which it is published in the official Gazette of [*insert name of Commonwealth member country*].

Exhibits to the Tiered Stablecoin Licensing Framework

Exhibit A:

1. Suggested Minimum Threshold Metric Table for Tier Classification

This illustrative Exhibit sets out the suggested minimum quantitative thresholds used to classify Issuers into different tiers.

Tier	Market capitalisation (US$ or currency equivalents)	Active user base	Average daily transaction volume (US$)	Cross-border usage
Tier 0	≤ 5 million	≤ 10,000	≤ 100,000	Not permitted
Tier 3	≤ 5 million	≤ 10,000	≤ 500,000	Minimal
Tier 2	5–500 million	10,000–1 million	≤ 100 million	Moderate
Tier 1	> 500 million	> 1 million	> 100 million	Extensive

2. Suggested Reserve Requirements for Stablecoin Issuers by Country

This illustrative chart sets out the suggested reserve requirement thresholds for Stablecoin Issuers across select countries. It includes minimum monetary thresholds, percentage reserve requirements and the 1:1 benchmark commonly used in regulatory frameworks.

Country	Reserve requirement type	Minimum threshold (US$ or currency equivalents)	Percentage requirement	1:1 benchmark statement
EU (MiCA)	Asset-backed	N/A	100%	Yes – full backing required on demand
UK (FCA)	Fiat-backed only	$2 million	100%	Yes – funds must be safeguarded 1:1 in a trust or client account
Bermuda	Asset-backed	$1 million	100%	Yes – must maintain reserves equal to outstanding tokens
Singapore (Payment Services Act)	Asset-backed	$1 million	100%	Yes – full value must be held in Segregated Accounts

Country	Reserve requirement type	Minimum threshold (US$ or currency equivalents)	Percentage requirement	1:1 benchmark statement
Hong Kong	Only fiat-backed permitted	$3 million	100%	Yes – fully backed and redeemable
Mauritius	Asset-backed	$500,000	100%	Yes – reserve assets must be equal to token liabilities
CML Stablecoin Model (draft)	Tiered by issuance level	Tier 1: $5 million Tier 2: $1 million Tier 3: discretionary	Tier 1: 100% + stress buffer Tier 2: 100% Tier 3: minimum 70%	Yes – 1:1 required at all tiers, with enhanced requirements at Tier 1

Exhibit B: Suggested Minimum Governance and Risk Control Checklist

This illustrative checklist details governance and risk control expectations by tier, including board composition, audit frequency, stress-testing and compliance functions:

Governance element	Tier 3	Tier 2	Tier 1
Board composition	Basic oversight	Non-executive board members	Independent majority
Risk committees	Optional	Recommended	Mandatory
Internal audit	Not required	Annual	Quarterly
Stress-testing	None	Annual	Biannual
Compliance officer	Mandatory	Mandatory	Mandatory

Exhibit C: Sample Technology and Cybersecurity Requirements

This illustrative Exhibit sets out a sample tier-based cybersecurity expectations, including SOC, audits and continuity plans:

Tier 3	Tier 2	Tier 1	Tier 0
Annual cybersecurity self-assessment	Annual integrity audit and self-assessment	Annual cybersecurity audit, red-teaming	Sandbox security plan with no public access unless tested
Regulator-issued technical checklist	Business continuity test	24/7 SOC and real-time monitoring	

Exhibit D: Sample Cybersecurity Assessment

This illustrative exhibit sets out sample baseline expectations by which issuers must conduct cybersecurity assessments, as follows.

(a) Network security controls (firewalls, intrusion detection)

(b) Access control and authentication mechanisms

(c) Incident response and recovery procedures

(d) Data encryption and secure storage

(e) Periodic penetration testing and vulnerability scans

(f) SOC monitoring

(g) Self-assessment reporting

Exhibit E: Sample White Paper Disclosure Structure

This illustrative exhibit guides issuers on the necessary content for user-facing White Papers.

(a) Executive Summary

(b) Stablecoin Mechanism and Peg Details

(c) Issuer Legal Entity and Governance

(d) Reserve Composition and Safeguards

(e) Redemption Process and User Rights

(f) Fees and Charges

(g) Risk Disclosures (market, operational, cyber)

(h) Audit and Transparency Policies

(i) Legal and Regulatory Disclaimers

(j) Contact Information and Complaints Handling

The Way Forward

The regulation of Stablecoins is entering a new phase, focused on institutional implementation, supervisory tooling and global co-ordination. Following the adoption of core legislative provisions – covering licensing, risk mitigation, Smart Contract security and cross-border standards – the next step involves operationalising these frameworks through transitional arrangements, regulatory guidance, sandbox mechanisms and stakeholder engagement. This approach balances innovation with integrity, ensuring scalable compliance and public trust in evolving digital financial ecosystems.

Delegated legislation

Commonwealth member countries may, depending upon their market maturity and regulatory readiness, customise this Model Law to the specific dynamics of their economies. This may be done by way of extensive and delegated legislation such as, among others, implementing regulations, guidance, circulars, rules, codes and FAQs. For example, the licensing application procedure, relevant timelines (and clock-stops, if any), administrative fees and penalties for non-compliance may be detailed in delegated legislation.

Follow-on amendments

While this Model Law may focus only on Stablecoins, as a class of VAs, there may be a need to amend other applicable laws to align them with the respective VA laws. This may include, *inter alia*, amendments to the applicable AML/CFT laws.

Ecosystem considerations

Notably, the world over, authorities and multilateral bodies are discussing the definitional challenges related to the digital economy. A key component of this debate is the definition of VAs. For example, FATF defines VAs as a digital representation of value that can be digitally traded, transferred or used for payment. Notably, it does not include digital representation of fiat currencies. Other components of the crypto ecosystem include DeFi, CBDCs, DAOs and Non-Fungible Tokens (NFTs), among others. Depending upon the market dynamics of each Commonwealth member country, regulatory frameworks could potentially factor in the nuances of each of these technologies and anticipate regulatory changes relating to them.

Sandbox

Commonwealth member countries may, by way of delegated legislation or regulatory initiatives, set up regulatory sandboxes and accelerator programmes to provide a secure testing environment for these emerging technologies. This can ensure these technologies are not unveiled to the world before end-to-end customer protection is guaranteed and comprehensive laws have been put in place. Commonwealth member countries may also consider setting up cross-border sandboxes and even sharing their learnings from sandboxing regimes by way of memoranda of understanding.

Other technologies

In a similar vein, the rapid advancement of AI technologies requires a dedicated legislative approach. As we witness the transformative potential of AI across various sectors, there is a growing need to establish comprehensive AI laws and regulations.

These regulations could encompass issues like the overlap of AI and blockchain technologies, AI and data privacy, AI and algorithmic accountability, and ethical AI development. Addressing these aspects within the framework of AI laws will be essential in shaping a responsible and innovative future for AI technologies within Commonwealth countries.

Annex: Committee of Experts

Kokila Alagh

Kokila Alagh is an expert in technology and corporate law in the Middle East. She is a thought leader on high-risk tech sectors such as fintech, financial services, VAs, gaming and AI.

She founded KARM Legal Consultants, an independent law firm that specialises in emerging tech, consulting fintech, VAs, data protection, AI and healthtech, advising multinationals, government and quasi-government entities within the Middle East and North Africa (MENA) region.

She is a Founding Member of the MENA Fintech Association, a Member of the Fintech Working Group Arab Monetary Fund and a Head Member of the Regulatory Vertical in the Dubai Digital Asset Association of Dubai Chamber of Digital Economy.

She studied in the Oxford Blockchain Strategy Programme at Oxford University, UK, and the Fintech Programme at Harvard Business School, US. She has an LLM in Digital Economy Law from Monash University, Australia, and an LLB (Hons) from Symbiosis Law School at the University of Pune, India.

Lieutenant Colonel Keron Burrell

Lt Col Keron Burrell is a senior financial regulator in Jamaica, responsible for market conduct and consumer protection supervision and for developing the country's regulatory framework for virtual and digital assets.

He previously served at the Bank of Jamaica, where he held several roles in the Policy and Methodology Department before becoming Chief Prudential Officer in the Financial Institutions Supervisory Division.

In parallel with his regulatory career, Lt Col Burrell has served in the Jamaica National Reserve since 2004 and currently commands the Third Battalion of the Jamaica Regiment National Reserve.

He holds an MSc in Accounting and a BSc in Economics and Accounting from the University of the West Indies and has contributed to international work on financial regulation and anti-money-laundering frameworks, including participation in the United Nations Commission on International Trade Law working group on secured transactions.

Stuart Davis

Stuart Davis is a banking executive with 35 years of experience and 21 years of specialisation in financial crime risk management in support of both business and regulatory objectives. He has served as a Special Advisor to the Chief Risk Officer at Toronto-Dominion Bank since July 2024.

He was Executive Vice President, Global Head of Financial Crimes Risk Management and Chief Anti-Money Laundering Officer (CAMLO) at Scotiabank, overseeing an AML/sanctions regulatory remediation that result in the lifting of two US written agreements. He subsequently served as Executive Vice President for Internal Data Protection, prior to a brief retirement.

Previously, he served as Senior Vice President, CAMLO and Global Head of AML for Bank of Montreal, leading on the lifting of two US written agreements.

He started his career with the Comptroller of the Currency.

Alexandra Delsol

Alexandra Delsol is a Venezuelan lawyer and founder of A2 Legal, a law firm dedicated to helping tech companies scale through tailored legal strategies. She was a 2023–2024 Chevening Scholar and a 2020 fellow of the Young Leaders of the Americas Initiative, and is a Global Shaper of the Caracas Hub.

She holds an LLM in Law & Technology from King's College London, UK, and an LLM. in Commercial Law from Universidad Católica Andrés Bello, Venezuela. She is also certified as a data protection lawyer by Universidad Javeriana, Colombia. Her practice focuses on the intersection of law, innovation and international growth.

Paul Derham

Paul Derham is Managing Partner of a leading Australian financial services regulatory law firm, advising global crypto and fintech companies.

He is also Chair of the Digital Economy Council of Australia, the country's apex industry body representing the digital asset sector.

Ankita Dhawan

Ankita Dhawan works at the intersection of law, public policy and business. She started her career at Google, where she worked on digital policy issues.

Currently at the Metis Institute, she advises governments, international financial centres and special economic zones around the world on the design of regulatory frameworks that enable emerging technologies and Stablecoins.

Previously, she worked in private legal practice in the United Arab Emirates and India, advising big-tech as well as startups on economic regulations at the intersection with technology, including antitrust, data protection and VAs.

She was a part of the drafting team for the Commonwealth Model Law on Virtual Assets.

Elizabeth Genia

Elizabeth Genia is Governor of the Bank of Papua New Guinea, the first woman to hold the position. She was appointed in December 2023 for a term of four years.

She has four decades of experience with the Bank, during which she has held several senior positions, including Department Manager, Assistant Governor and Acting Governor, a role she held for 12 months. She has also served for many years as a Member of the Bank's Executive Committee.

Her work has focused on financial technology, financial inclusion and gender equity. Under her leadership, the Bank developed a world-first identity confirmation technology to support financial inclusion in Papua New Guinea.

Previously, as Assistant-Governor for Corporate Affairs, she led the development and implementation of the Bank's Gender Equity and Social Inclusion Policy.

She has broad business experience in finance, auditing, corporate governance, strategic planning, risk management, administration and policy development.

She holds an MBA from the University of Queensland, Australia; a Graduate Certificate in the Fintech Programme from Said Business School, University of

Oxford, UK; a Graduate Certificate in Management and Organisational Change, Australian National University; and a Bachelor of Commerce from the University of Papua New Guinea.

Jonathan Hatch

Jonathan Hatch is a lawyer, regulator, academic and adviser with over two decades of experience spanning financial services, technology regulation and industry practice. His background includes extensive work supporting startups and scale-ups, particularly in navigating complex regulatory environments.

He specialises in emerging technologies, with a focus on blockchain and AI. He has taught at the University of Sydney, the Royal Melbourne Institute of Technology and other leading Australian institutions, as well as the London School of Economics and Political Science. He also contributes to international capacity-building on technology policy and represents Australia in the development of ISO standards, with a particular emphasis on AI governance, risk and responsible deployment.

Marc Krisjanous

Marc Krisjanous is Associate Director of Audit at SixBlocks Audit, which provides assessment and audit services to the web3 sector worldwide. He is a Member of the Executive Council of Blockchain New Zealand, a member of the CCSS Steering Committee and a New Zealand expert and co-editor for ISO TC307.

He has worked in the information security sector for over 15 years, with 10 years as an auditor. He audits under CCSS, ISO/IEC 27001 and PCI DSS, conducting third-party risk assessments for insurance providers and other stakeholders and advising governments worldwide on web3 cybersecurity.

He contributes to the creation of several standards, including ISO TC307 (the ISO standards for blockchain and DLT systems), CCSS (a key management standard for blockchain and DLT systems) and Singapore Baseline Security Requirements for Blockchain and DLT Systems.

He educates the web3 community on cybersecurity through speaking engagements, webinars and published articles. He also authored the CCSS v9 Implementation Guide.

Louise Malady

Louise Malady is a policy adviser with 25 years of experience across payments and financial prudential regulation. She has worked as a consultant and academic researcher in fintech, and has done extensive fieldwork, providing technical assistance to financial regulators in emerging markets.

She is currently working in aged care reform enabling academics working on transdisciplinary complex problems to improve the policy impact of their work to address the challenge of making aged care economically, socially and environmentally sustainable. In her spare time, she closely follows and advocates for the safe development of digital money and using technology to improve the accessibility and navigability of financial laws and regulations.

Ian Matthews

Ian Matthews is a legal expert in financial services and supervisory and beneficial ownership aspects of AML/CFT. He previously worked at the Financial Conduct Authority in the UK as a specialist in international AML/CFT matters. He spent two years on secondment to the European Commission, where he worked on drafting the EU's Fourth Anti-Money Laundering Directive.

He was Co-Chair of FATF's Evaluations and Compliance Group, which is responsible for overseeing the conduct of the global mutual evaluation process, and is currently a Scientific Expert for the Council of Europe's MONEYVAL Committee. He has an LLB from Manchester Metropolitan University, UK, and trained as a solicitor at the College of Law, York, UK.

Rick McDonell

Rick McDonell is a Co-Chief Executive Officer of McDonell-Nadeau. He is also Executive Director of the Association of Certified Anti-Money Laundering Specialists. His work as Executive Secretary of FATF has included FATF's revision of the international AML/CFT/PF Standards, the new Mutual Evaluation methodology covering technical and effectiveness compliance and expansion of the FATF Global Network to nine FATF-Style Regional Bodies.

Prior to his FATF role, he was Chief of the UN Global Programme against Money Laundering and the founder and inaugural Executive Secretary of the Asia-Pacific Group on Money Laundering.

He has extensive experience as a prosecutor and investigator leading complex multidisciplinary investigation taskforces into organised crime cases both nationally and internationally.

He is Chair of the Advisory Board on the Future of Financial Intelligence Sharing. He is a graduate of Monash University, Australia, with a BA, LLB and Graduate Diploma in Commercial Law.

Harvesh Kumar Seegolam, GCSK

Harvesh Kumar Seegolam served as Governor of the Bank of Mauritius from 2020 and Chairperson and Chief Executive of the Financial Services Commission of Mauritius.

He has more than 15 years of experience in financial sector policy and development, contributing to initiatives aimed at strengthening Mauritius as an international financial centre.

As Governor during the Covid-19 pandemic, he oversaw monetary and financial system responses to the global economic disruption. In 2024, he was elected President of the Association of African Central Banks in 2024.

His work has included the development of Mauritius' fintech strategy, VA legislation, the new monetary policy framework adopted in 2023 and cross-border payment links between Mauritius and India, and the establishment of Mauritius as an RMB clearing centre.

He has also led initiatives to strengthen AML/CFT frameworks and overseen the creation of the Bank of Mauritius Innovation Hub and the Bank of Mauritius Climate Change Centre.

He now works independently on financial innovation, cross-border payments and regulatory frameworks.

Lord Anthony St John

Lord St John of Bletso took up his seat as a Crossbench Member of the House of Lords in 1978.

He was brought up in South Africa, where he qualified as an attorney before working for Shell as an internal auditor and legal counsel.

He completed his Master's degree in Law at London University, UK, specialising in Chinese and Maritime Law, and spent a year living in China and Hong Kong in 1983. He worked for over 15 years in financial services in London, initially as an oil analyst and then in equity sales and investor relations with Smith New Court and then Merrill Lynch, focusing on Sub-Saharan Africa and the Far East.

Lord St John was appointed Extra Lord-in-Waiting to Her Majesty The Queen in 1998. He currently serves on the House of Lords Space Economy Select Committee.

Jane Thomason

Jane Thomason is a globally recognised thought leader, entrepreneur and futurist, working at the intersection of technology and social impact. She serves on the editorial boards of *Global Health Journal*, *Frontiers in Blockchain* and *Journal of Metaverse*.

She has authored multiple books, including *Blockchain Technologies for Global Social Change Applied Ethics in a Digital Age* and *Advancements in the New World of Web 3: A Look Toward the Decentralized Future*. She has published widely on medtech, web3, blockchain, AI and the metaverse.

She serves as Chair of Kasei Digital Assets, a company listed on the Aquis Exchange in London, focusing on investments in digital assets and blockchain technologies.

Siddharth Tiwari

Siddharth Tiwari has more than three decades of experience in international financial policy and senior leadership roles in global financial institutions, working across five continents. He is currently on the Advisory Council of the Bretton Woods Committee, Washington, DC, US; a Fellow at Chatham House, London, UK; and Vice-President of the International Finance Forum, Beijing, China.

He has served as Senior Advisor to India's G20 Presidency; headed the BIS Asia and Pacific Office in Hong Kong; taken on the role of Executive Secretary of the G20 Eminent Persons Group in Singapore; and worked in the IMF as Director of Strategy Policy and Review, Secretary of the IMF, Chief of Staff for the Managing Director and Head of Country Operations in Africa, among others.

In these roles, he has spearheaded efforts to reform the international monetary and financial system, integrating advances in technology with finance with a focus on the governance of the system; shaped institutional responses to mitigate the adverse impact emanating from the global commons (pandemic and climate); led the strategy and design of global financial architecture; directed policy and lending operations; managed a large international board of directors; implemented deep institutional restructuring; headed multibillion dollar investment committees; and, managed billion-dollar budgets.

With substantial global experience in Asia, he has led engagements between and within international bodies (G7 and G20), the public sector, think-tanks, philanthropic foundations, civil society, financial markets, the media and academia.

He holds degrees in Economics from the University of Chicago, US; the London School of Economics and Political Science, UK; and the University of Delhi, India.

Muazu Umaru

Muazu Umaru, a Nigerian national, currently serves as Director of Policy & Research at the Inter-Governmental Action Group against Money Laundering in West Africa – an FATF-Style Regional Body under the Economic Community of West African States, headquartered in Dakar, Senegal. He is internationally recognised expert in countering

organised crime, financial crime, money laundering and terrorist financing and in counter-narcotics.

He began his professional career in 1997 as a trained counter-narcotics officer with Nigeria's National Drug Law Enforcement Agency, where served as Head of International Affairs and Special Assistant to the Chair/Chief Executive.

He has led and supported numerous initiatives, including risk assessments, strategies and actions plans related to AML/CFT; building capacity for the effective implementation of FATF standards; supervising research on emerging threats and vulnerabilities in financial systems; and global policy work for FATF for over 16 years. He also has a longstanding interest in the intersection of technology, financial systems and crime prevention.

He was Chevening Fellow (2009), with a focus on organised crime and governance, and U.S. State Department International Leadership Visitor Program Fellow (2003), with a focus on transnational crime and law enforcement co-operation.

With his strategic insight, commitment to research and reform, and a wealth of experience, Mr. Umar continues to be a leading figure in shaping effective responses to financial crime and terrorism financing in West Africa and globally.

Joseph Weinberg

Joseph Weinberg is a digital asset pioneer and co-founder of Shyft Network, which leverages blockchain and Smart Contract infrastructure to achieve greater standardisation and efficiency in regulatory compliance and due diligence mandates. Joseph was a pioneer bitcoin miner and has helped progress the VA industry while also advocating for sound policy and regulatory requirements globally.

He serves as an adviser to the Organisation for Economic Co-operation and Development, FATF, governments and regulatory bodies globally. Through his work at the Organisation for Economic Co-operation and Development, he is helping draft global policies for the G7 and G20 councils and drafted the first digital asset regulations globally. He is also an active adviser for the Ontario Securities Commission and the Investment Industry Regulatory Organization of Canada.

He is co-founder and Chief Executive Officer of Paycase Financial, a value network and trust-ware provider for decentralised financial services.

Prior to pioneering the first companies in the digital asset ecosystem, he worked in roles at both Xtreme Labs and Pivotal Inc., building some of the largest mobile applications currently in use around the world today, including Uber, Facebook and Airbnb.

Jeff Yew

Jeff Yew is founder and Chief Executive Officer of Monochrome, a crypto-asset financial services company in Australia.

Monochrome's asset management arm is the investment manager of Australia's first in-kind spot Bitcoin exchange-traded fund.

Previously, he was the founding Chief Executive Officer of Binance Australia, the country's largest digital currency exchange by trading volume during his tenure.

Anson Zeall

Anson Zeall is a blockchain compliance strategist who guides regulators and high-growth crypto firms across Asia, Europe and the US. As founder and Managing Director of Azentiq Nexus, he helps leadership teams weave compliance into product strategy and market expansion

Previously, he served as Chief Strategy Officer and Head of Compliance at dtcpay, steering multi-country licensing initiatives and audit readiness. An early pioneer, he co-founded CoinPip – one of Southeast Asia's first blockchain payment platforms – shaping discussions that informed Singapore's early crypto regulations .

He also chairs ACCESS, Singapore's industry association for blockchain enterprises, leading dialogue with policymakers on digital asset standards, and hosts The Zeall Show, a livestream series featuring conversations with global fintech and regulatory leaders.

Wei Zhou

Wei Zhou is Chief Executive Officer of Coins.ph, the Philippines' largest regulated cryptocurrency exchange, with 18 million customers. He is leading global expansion through Coins.xyz into Australia, Europe, Latin America and Africa.

Before Coins, he was Chief Financial Officer at Binance, guiding it to become the world's largest exchange, and served as Chief Financial Officer at Zhaopin.com and Charm Communications. He also led the landmark acquisition of Grindr, where he served as Vice Chair.

Drafting team

Maxine L. Binns

Maxine L. Binns is a barrister and attorney with expertise in corporate, commercial and estate law. She has worked with several local law firms and banking institutions and has over 40 years private industry experience.

More recently, she held the position of Legislative Analyst and subsequently Legislative Consultant with the Bermuda Government, where she contributed to economic business development, policy formulation and the advancement of private and public legislative initiatives. She collaborated closely with local and international agencies to modernise and enhance Bermuda's offerings as a international financial centre, while ensuring compliance with international standards. Notable outcomes of these efforts include the implementation of Bermuda's economic substance and digital asset business regimes.

She is a former Member of both the Human Rights Board of Inquiry and, more recently, the Commission of Inquiry into Historic Land Losses in Bermuda.

She read Law at the University of Buckingham and BPP Law School, UK, and was admitted to both the Bar of England and Wales and Bermuda Bar.

She was a Member of the Commonwealth Committee of Experts supporting the Commonwealth Working Group developing the Model Law on Virtual Assets.

Loretta Joseph

Loretta Joseph is an expert legal adviser with over 25 years' experience in financial services. She has served on boards and held senior roles in major investment banks across Asia and India, such as Royal Bank of Scotland, Macquarie Group, Deutsche Bank, Credit Suisse and Elara Capital. Her extensive career has provided her with deep exposure to global financial markets, various asset classes and emerging market environments.

She has advised various countries, including Mauritius, Bermuda, Serbia and Vanuatu, on developing legal and regulatory frameworks for virtual assets. She has also advised the Organisation for Economic Co-operation and Development and the Organization

for Security and Co-operation in Europe, and is an expert industry participant in many international standard-setting bodies concerning the adoption of VAs. Her contributions in these areas have been pivotal in guiding global policy and regulatory approaches to digital finance. She is Co-Chair of the International Digital Asset Exchange Association.

She was a Member of the Commonwealth Committee of Experts supporting the Commonwealth Working Group developing the Model Law on Virtual Assets.

Yvan Jean-Louis

Yvan Jean-Louis is Assistant Solicitor-General in the Office of the Attorney General in Mauritius. He previously served as Senior State Counsel and Assistant Parliamentary Counsel. He is Head of the International Trade Unit at the Attorney-General's Office responsible for international trade, international co-operation in criminal matters (extradition, mutual legal assistance and transfer of prisoners), taxation and financial services, among others.

He currently represents the Government of Mauritius on the Board of the Mauritius International Arbitration Centre. He also served as a Member of the National Regulatory Sandbox Licensing Committee responsible for licensing fintech startups in Mauritius from 2019 to 2021. He is also Vice-Chair of the Financial Services Review Panel, which hears appeals against administrative sanctions imposed on licensees of the Financial Services Commission.

He holds an LLB (Hons) from the University of Buckingham, UK, and an MSc in Law and Accounting from the London School of Economics and Political Science, UK. He also holds a Postgraduate Diploma in Legislative Drafting.

He was a Member of the Commonwealth Committee of Experts supporting the Commonwealth Working Group developing the Model Law on Virtual Assets.

Susan Jarvis

Susan Jarvis is a former educator with 10 years' experience teaching English, literature, business and business law. She later obtained an LLB from Nottingham Law School, UK, and pursued a legal career focused on legislative drafting and the development of legal frameworks in Antigua and Barbuda and internationally.

Susan holds a PG Dip. from Athabasca University, Canada, and an LLM from the University of the West Indies in Legislative Drafting. She has been actively drafting legislation on a national and regional level for over 10 years and has followed the progression of laws she has drafted through multiple parliamentary sessions. She is currently employed at the Commonwealth Secretariat as a Legal Adviser for Legislative Support and Law Reform. Prior to joining the Secretariat, she was Antigua and Barbuda's Law Revision Commissioner and managed the law consolidation and revision project.

Susan is called to the Bar of England and Wales and Antigua and Barbuda.

The Commonwealth

D20423