FINANCIAL SERVICES AUTHORITY
SAINT VINCENT & THE GRENADINES

GUIDELINES:

VIRTUAL ASSETS BUSINESSES

IN

ST. VINCENT AND THE GRENADINES

Contents

GLOSSARY OF TERMS

Term	Definition
Auditor	Has the meaning assigned under Section 12 of the Virtual Assets Business Act. Typically, a professionally certified individual or firm authorized to independently assess and report on a registrant's financial and operational integrity.
Beneficiary	The natural person, legal person, or legal arrangement that will ultimately receive or own the virtual asset upon completion of a transfer.
Beneficial Owner	As defined under Regulation 4 of the Anti-Money Laundering and Terrorist Financing Regulations 2014. Includes any natural person who ultimately owns or controls a registrant, or on whose behalf a transaction is conducted
Certified Information Systems Auditor (CISA)	A globally recognized IT audit designation issued by ISACA. Required for professionals who assess internal controls, cybersecurity, and compliance with information systems policies.
Client	A person with whom a virtual asset business establishes or intends to establish business relations, or for whom it undertakes or intends to undertake a transaction.
Customer Due Diligence (CDD)	The process of verifying the identity of a client and assessing the risk they pose in accordance with AML/CFT requirements. Includes KYC (Know Your Customer) checks and ongoing monitoring.
Decentralized Application (DApp)	A blockchain-based application that runs autonomously and is not controlled by a central authority. Often used in DeFi services and powered by smart contracts.
Escrow	A contractual arrangement in which a third party temporarily holds software code, funds, or other assets on behalf of transacting parties until a condition is met. Used for proprietary software protections.
Fit-and-Proper Criteria	A standard for assessing the integrity, competence, financial standing, and regulatory history of individuals such as directors, shareholders, and officers. Typically includes checks on criminal records, conflicts of interest, and professional conduct.
Market Abuse	Conduct involving manipulation of the virtual asset markets, including insider trading, false disclosures, price manipulation, and

	dissemination of misleading information.
Non-Custodial Wallet	A digital wallet where only the user has control over their private keys and assets. The service provider cannot access, freeze, or transfer funds on the user's behalf.
Originator	The natural person, legal person, or legal arrangement that places a transfer order. If the transfer is executed by a registrant on behalf of a client, the originator is the person who owned the asset before the transaction.
Proprietary Software	Software developed and owned by a registrant or third-party vendor, typically forming part of its core business operations (e.g., a private trading engine or custody wallet platform). May be subject to escrow requirements under IT audit rules.
Ring-Fencing	The legal and operational separation of client assets from a VAB's own corporate funds. Designed to protect customer assets in the event of insolvency, fraud, or litigation. Required under Regulation 21.
Risk Appetite	The amount and type of risk that an organization is willing to accept in pursuit of its objectives. Must be clearly defined and linked to the entity's risk management framework.
Statutory Deposit	A regulatory reserve held by VABs with a licensed bank or in approved securities, pledged to the FSA. Ensures protection against solvency risks and client obligations.
Smart Contract	A self-executing contract with the terms directly written into code and deployed on a blockchain network. Triggers automatic transactions once predefined conditions are met.
Technology Platform	A digital interface or software infrastructure provided by a VAB to facilitate the sale, trading, exchange, or transfer of virtual assets. Examples include centralized exchanges or peer-to-peer trading platforms.
Transfer of Virtual Asset	The process of moving a virtual asset from one account or address to another, usually executed on behalf of a client (originator).
Virtual Asset (VA)	A digital representation of value that can be digitally traded or transferred and used for payment or investment. Includes cryptocurrencies, certain NFTs, and stablecoins. Does not include fiat currency or traditional securities.

Virtual Asset Business	Any business activity conducted in connection with virtual assets including exchange, transfer, custody, issuance, or related financial services.

1. Introduction

These Guidelines are issued by the Financial Services Authority (FSA) pursuant to section 23 of the *Virtual Asset Business Act*, No. 9 of 2022 (the "Act")

The purpose of these guidelines is to establish minimum prudential, operational, and compliance requirements for registrants engaging in virtual asset business in or from St. Vincent and the Grenadines (SVG).

2. Scope and Applicability

2.1 In accordance with the Act, a Virtual Asset Business (VAB) refers to the conduct of any of the following activities on behalf of another person:

i) Exchange between virtual assets and fiat currency.
ii) Exchange between one or more forms of virtual assets.
iii) Transfer of a virtual asset, whether or not for value.
iv) Safekeeping or administering of a virtual asset or instruments enabling control over a virtual asset.
v) Participating in or provision of financial services related to the issue or sale of a virtual asset.

2.2 The following are examples of VABs:

- A **crypto exchange** (*platform which facilitates the buying, selling, or trading of virtual assets (crypto-to-crypto or crypto-to-fiat)*). E.g. the offering of spot trading of Bitcoin and Ethereum

- A **crypto transfer service** (*a service which allows for the sending or receiving of cryptocurrency*)

- A **crypto wallet provider** (*a platform which offers hosted wallets and involves the custodial control of user's keys*)

- A **cryptocurrency issuer** (*a company which issues or creates virtual assets such as tokens, stablecoins, NFTs, as a business*)

- A **crypto payment processor** (*a service allowing businesses to accept cryptocurrency payments*)

- **crypto custodian** (*a company that securely stores virtual assets*) E.g. offering custody solutions to high-net-worth individuals or institutions investing in crypto

- A **crypto payroll service** (*a company which pays employees in cryptocurrencies*)

2.3 The following are **not** a VAB:

- A company which only provides technology (e.g. cloud storage for crypto data).
- A private individual making a one-time crypto transfer.
- A business using cryptocurrency for its own transaction only.

*****Entities or platforms not controlling customer funds or private keys (e.*g., pure technology developers, non-custodial wallet providers, or fully decentralized apps*) may not be classified as VAB under the Act but may be subject to scrutiny by the FSA on a case-by-case basis.**

2.4 Examples of virtual assets include:

- Cryptocurrencies (Bitcoin (BTC), Ethereum (ETH), Solana (SOL)
- Stable coins (Tether (USDT), pegged to fiat currencies
- Some Non-fungible tokens (NFTs)- if the NFT is used for payment or investment rather than as a digital collectible

2.5 For the avoidance of doubt, the following are **not** virtual assets:

- Fiat currency (USD or ECD) stored in a bank account
- Securities stock and bonds
- NFTs that serve only as collectibles and not as means of payment[1] or investments[2]. For the purposes of this section, NFTs (non-fungible tokens) shall be considered virtual assets when they are used as a medium of exchange, a unit of account, or store of value, particularly if:
    - the NFT can be traded or exchanged on a secondary market.
    - it represents a fractionalized interest in a revenue-generating asset (e.g., real estate, securities).
    - it derives value from speculative investment or profit expectation, similar

[1] Example (Means of Payment): A gaming NFT used to buy in-game upgrades across a network of interoperable games may qualify as a virtual asset used for payment.
[2] Example (Investment): An NFT offering a share of streaming revenue from a song or video, marketed with promises of returns, may be considered an investment.

to security tokens."

*****A further description of VAB activities are outlined in Annex 1.**

3 Registration Requirements for Virtual Asset Businesses

3.2 Any person seeking registration as a VAB must submit a written application to the FSA accompanied by all required information and documents as outlined in Section 6 of the Act and Regulation 3 of the Virtual Asset Business Regulations ("The Regulations").

3.3 An entity that submits an application to the FSA will be required to provide information and documents as outlined in the Act, the Regulations, and any additional Guidance issued by the FSA. The FSA may request further information during the review and authorization process, including details on corporate governance, AML/CFT compliance, risk management, and cybersecurity protocols.

3.4 Registrants must comply with the fit-and-proper criteria established under section 7(2)(a) of the Act, ensuring that directors, officers, beneficial owners, and principal representatives meet FSA's integrity, financial standing, and competence standards.

3.5 VABs will be required to pay an application fee and registration fee in accordance with Schedule 1 of the Act. Failure to maintain valid registration may result in regulatory enforcement action, including suspension or revocation of the registration pursuant to Section 18(1) of the Act.

3.6 VABs must obtain prior approval from the FSA before undertaking any sale, transfer, merger, acquisition, or amalgamation of its business interests, assets, shares, or operations, either wholly or partially, with any other entity. This requirement ensures regulatory oversight of structural changes that may impact financial stability, compliance, and consumer protection.

3.7 Only VABs registered by the FSA are permitted to offer Virtual Asset Services in or from within SVG. Engaging in virtual asset business activities without being registered under the Act is an offence pursuant to Section 19 of the Act and will result in penalties, fines, and potential imprisonment.

4 Application for Registration

4.2 In considering an application for a licence, the FSA shall conduct such investigation as it deems necessary to ascertain:

(a) The authenticity and completeness of submitted documents;
(b) The financial condition, solvency, and track record of the applicant.
(c) The nature and scope of the virtual asset business.
(d) The source and legitimacy of initial capital and proof of funding.
(e) The relevance of the proposed services to the development and stability of SVG's financial sector.
(f) The fitness and probity of the applicant's beneficial owners, shareholders, directors, officers and management team.

4.3 In determining whether an applicant is a fit and proper person, the FSA shall assess the following criteria for each of the applicant's beneficial owners, significant shareholders, directors, executive management, and officers:

- educational background, qualifications and relevant experience;
- reputation, integrity and history of regulatory compliance;
- any prior criminal, civil, or regulatory sanctions;
- financial soundness and history of all associated parties[3], including beneficial owners, directors, officers, and affiliated entities.

4.4 The FSA may also take into account the financial and compliance status of any associated persons or entities, including:

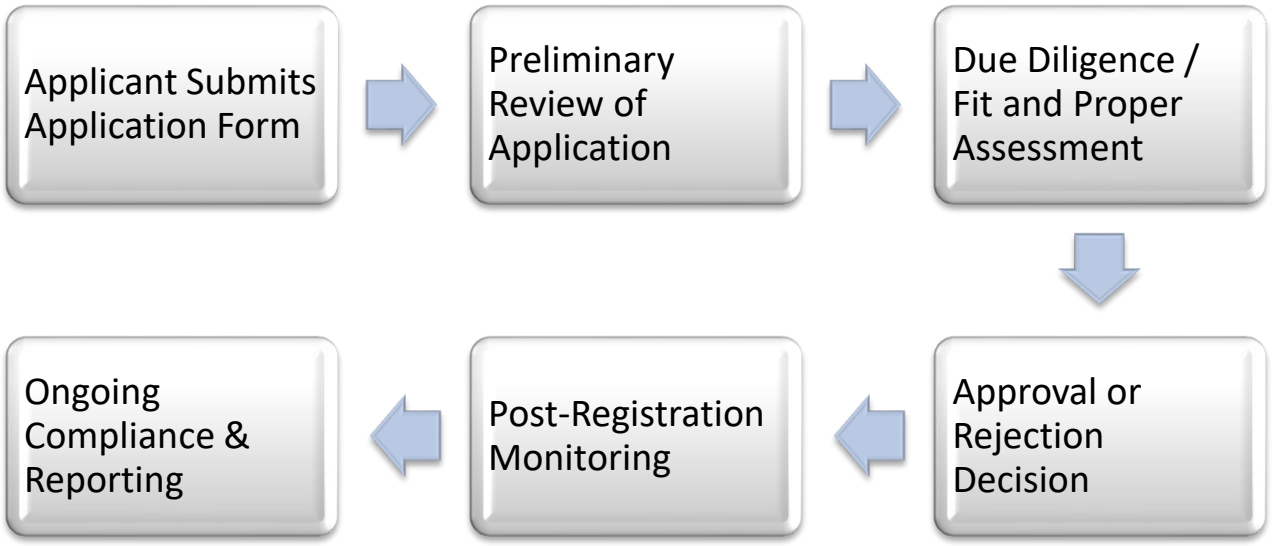
- any individual who will be employed by or associated with the applicant in connection with the virtual asset business.
- any agent, principal representative, or third-party service provider associated with the business.
- any significant shareholder, director, officer, or affiliated entity, including their regulatory history and financial standing.
- financial health, capital adequacy, and solvency of the applicant's beneficial owners and shareholders, ensuring compliance with capital and liquidity requirements under the Regulations.

4.5 The FSA may reject an application or impose conditions on registration where

[3] "Associated persons or entities may include but are not limited to:
- External auditors conducting financial or compliance reviews;
- Custodians safeguarding customer virtual assets or private keys;
- Third-party technology vendors providing trading engines, APIs, or custodial infrastructure;
- AML/CFT compliance consultants;
- Affiliate or parent companies with operational or ownership links to the registrant.

deficiencies are found in governance, risk management, or AML/CFT frameworks.

VAB REGISTRATION PROCESS



5 Core Financial requirements for Virtual Asset Businesses

Capital Requirements

5.2 VABs are required to maintain a minimum paid-up capital of **EC$50,000** and an authorized capital of **EC$300,000**.

5.3 Notwithstanding the above, VABs may be required to maintain higher levels of capitalization based on the FSA's assessment of the nature, size, and risk exposure of the licensee's operations. The FSA reserves the right to impose additional capital adequacy requirements based on market volatility, business model, and operational complexity.

Statutory Deposit requirement

5.4 Registered VABs are required to maintain a minimum statutory deposit of **EC$100,000 or an amount equal to 25% of the financial obligations to clients of the registrant, whichever is greater,** with a bank licensed under the Banking Act, 2015.

5.5 The statutory deposits may be made in cash, government securities or in any

other approved form. **Annex 2** outlines the acceptable form of securities which may use as Statutory Deposits in lieu of cash.

5.6 The statutory deposit shall be pledged to the FSA as trustee.

5.7 Failure to maintain the deposit may result in regulatory sanctions, suspension, or revocation of the license under Section 18 of the Act.

Customer Fund Coverage

5.8 Registered VABs that have custody of virtual assets for clients are required to maintain an amount that is larger than the obligations of the VAB to the client in accordance with Regulation 10 of the Regulations.

5.9 Registrants must safeguard funds received from clients by ensuring they are kept separate and not commingled with its own or other funds in accordance with Regulation 21 of the Regulations.

6 Governance for Virtual Asset Business Providers

Governance

6.2 VABs shall establish effective and transparent governance arrangements to ensure the integrity and security of operations. At a minimum, governance arrangements shall include:

(a) processes to ensure that beneficial owners, shareholders, directors, managers, and agents meet the fit-and-proper criteria

(b) clearly defined and documented organizational arrangements, including:

- A formalized management structure with clear lines of accountability.
- Well-defined responsibilities for key personnel in significant positions.
- Proper personnel management and succession planning arrangements to ensure business continuity.

(c) Corporate governance policies and incorporation documents that outline the scope of the virtual asset business, including policies governing AML/CFT compliance, customer proception, data protection and cybersecurity.

Risk management framework

6.3 VABs shall implement comprehensive risk management frameworks to ensure the safety and integrity of their operations. These arrangements must include:

(a) Identification and assessment of risks associated with virtual asset transactions, financial services, and business operations.
(b) A risk management policy and internal control framework with documented procedures and systems to identify, measure, and monitor risks.
(c) A customer risk management plan, including measures to mitigate market, operational, liquidity, cybersecurity, and fraud risks.
(d) Liquidity and capital management strategies to ensure sufficient financial reserves in compliance with capital adequacy requirements.
(e) A compliance function to monitor regulatory obligations, AML/CFT compliance, and cybersecurity controls.

Operational policies and procedures

6.4 VABs must establish appropriate operational policies and procedures, including:

(a) Rules, policies, procedures, and agreements outlining the contractual rights and obligations of third-party service providers, merchants, sub-agents, and customer.
(b) Measures to ensure the security, safety, and reliability of platforms and transactions, including disaster recovery and contingency plans
(c) Interoperability mechanisms to ensure seamless integration with global virtual asset networks and financial service provider
(d) Accurate and complete record-keeping of transactions and customer accounts to ensure financial transparency and compliance with the FSA's reporting requirements
(e) Terms and conditions for service use, which must be accessible, transparent, and easy to understand for customers.
(f) Escrow requirements for proprietary software, ensuring no unauthorized system changes occurs post-audit.

6.5 Prior to the commencement of operations, VAPs must conduct a comprehensive IT audit, which must be performed by a Certified Information System Auditor (CISA). Periodic IT audits must be submitted to the FSA to demonstrate ongoing compliance with data security, cybersecurity protocols, and risk mitigation strategies. All IT audits must include an assessment of system vulnerabilities, penetration testing, and

disaster recovery plans to ensure operational resilience.

7 Cybersecurity, Data Protection, and IT Governance

7.2 Cybersecurity Audits

- Under Regulation 18(4) of the Regulations, all registrants must submit an annual independent cybersecurity audit.
- The audit must assess IT system vulnerabilities, data security controls, incident response plans, and compliance with best practices.
- The FSA reserves the right to require additional audits if deficiencies are identified.

7.3 Data Protection and Privacy

- Registrants must have strong encryption, access controls, and secure data storage for client information.
- Personal data must be processed in line with the St. Vincent and the Grenadines Data Protection Act and international data security standards.
- Any data breach must be reported to the FSA within 48 hours of detection.

7.4 IT Governance Framework

- Registrants must establish internal policies, procedures, and technical controls that align with international best practices such as ISO 27001, NIST Cybersecurity Framework.
- A designated Chief Information Security Officer (CISO) must oversee IT security governance.

7.5 AML/CFT Policies and Procedures

Registrants must establish internal policies, procedures, which outlines their commitment to preventing money laundering and terrorist financing in accordance with local and international standards.

8 Outsourcing Requirements for Virtual Asset Business Providers

8.1 Outsourcing of managerial functions is strictly prohibited.

8.2 VABs intending to outsource operational functions must obtain prior approval from the FSA. The application for authorization must include:

- Identification and details of the outsourcing entity, including its location and business activities.
- Risk assessments outlining how outsourcing may impact compliance, security, and operational efficiency.

8.3 The FSA will only approve outsourcing arrangements if the following conditions are met:

- Outsourcing must not result in the delegation of senior management responsibilities.
- Internal controls must not be weakened by outsourcing.
- Customer rights and obligations must remain unchanged.
- Outsourcing arrangements must not conflict with FSA's registration conditions.
- The outsourcing arrangement must not hinder FSA's ability to conduct oversight or enforce compliance requirements.

8.4 VABs continue to remain fully liable for the decisions and actions of entities to which functions have been outsourced.

9. Registration of Merchants and Agents

A merchant or agent may be considered for a virtual asset business license only if it meets the following conditions:

9.1 **Partnership with a well-established, regulated exchange:**

- The exchange must be licensed and regulated in a jurisdiction with AML/CFT compliance recognized by the FSA.
- The FSA reserves the right to deny approval if the partner exchange lacks transparency or regulatory oversight.

9.2 **Availability of Financial Information from the Exchange:**

- The exchange must file audited financial statements with the FSA within three (3) months of the end of the financial year in accordance with section 12 (3) of the Act,
- Proof of reserves, and liquidity reports must be provided to the FSA upon request.
- The FSA must be able to verify the solvency and capital adequacy of the exchange.

9.3 Ability to Enter into an MOU with the Exchange's Regulator:

- The FSA must be able to establish regulatory cooperation agreements (e.g., Memoranda of Understanding - MOU) with the financial regulator overseeing the exchange.
- This is critical for information-sharing, enforcement actions, and cross-border compliance.

9.4 Disclosure of Ultimate Beneficial Owners (UBOs):

- The exchange must disclose its ultimate beneficial owners (UBOs) to the FSA.
- The FSA will conduct fit-and-proper assessments

10. Ongoing Compliance Obligations

10.1 Reporting Requirements

- Registrants must submit quarterly financial reports to the FSA. The reports should include details on income, expenses, proof of funds and solvency. Proof of funds and solvency reports must demonstrate continuous coverage of customer liabilities.
- Registrants must submit audited financial statements prepared in accordance with international accounting standards.
- Any suspicious transactions must be reported immediately to the Financial Intelligence Unit (FIU).

10.2 Customer Protection and Risk Management

- Registrants must develop and implement a customer protection policy which includes complaint handling procedures and ring-fencing of client funds.
- Registrants must maintain internal risk management frameworks to mitigate operational, liquidity, and cybersecurity risks.

10.3 AML/CFT Compliance

- Registrants must comply with AML/CFT Regulations and implement:
    - Customer Due Diligence (CDD)
    - Enhanced Due Diligence (EDD) for high-risk clients
    - Transaction monitoring and reporting

11. Enforcement and Sanctions

11.1 The FSA may take enforcement action, including:

- Administrative penalties for breaches of compliance obligations.
- Suspension or revocation of a license for failure to meet capital, cybersecurity, or reporting requirements.
- Legal proceedings for regulatory non-compliance, including monetary fines and imprisonment under Section 19 of the Act.

12. Conclusion

The FSA is committed to fostering a safe, secure, and compliant virtual asset sector in St. Vincent and the Grenadines. These guidelines serve to protect consumers, mitigate financial crime risks, and ensure regulatory transparency in the virtual asset business industry.

ANNEX 1 - EXAMPLES OF THE DIFFERENT ACTIVITIES UNDER THE DEFINITION OF VIRTUAL ASSET BUSINESS

The following are examples of the different activities under the definition of **Virtual Asset Business**, in keeping with the Virtual Asset Business Act:

1. Exchange between a virtual asset and fiat currency

A company engages in this activity if it facilitates the conversion of cryptocurrency into fiat currency (e.g., XCD, USD, EUR) and vice versa. Examples include:

(a) A cryptocurrency exchange registered in SVG that allows users to buy Bitcoin or other types of cryptocurrency using Eastern Caribbean Dollars.

(b) A retail business that accepts cryptocurrency as payment and provides an in-store crypto-to-fiat exchange service.

(c) A crypto ATM operator that installs Bitcoin ATMs in SVG, allowing customers to withdraw XCD in exchange for Bitcoin.

(d) A brokerage firm that helps clients convert their digital assets into cash or vice versa.

(e) A local merchant who assists customers in funding their cryptocurrency exchanges account in exchange for cash or bank transfers.

(f) An individual or small business that facilitates peer-to-peer (P2P) transactions by matching buyers and sellers and handling the fiat settlement.

---

2. Exchange between one or more forms of virtual assets

This occurs when a company facilitates crypto-to-crypto trading, allowing customers to exchange one form of digital asset for another. For example:

(a) A crypto exchange platform that enables users to swap Bitcoin (BTC) for Ethereum (ETH) or Tether (USDT) for Solana (SOL).

(b) A crypto trading desk that provides over-the-counter (OTC) services, allowing high-net-worth and other clients to exchange large amounts of one crypto for another.

(c) A blockchain gaming company that allows players to convert in-game tokens into other digital assets.

(d) A merchant or individual who assists users in exchanging stablecoins (e.g., USDT) for other cryptocurrencies like Bitcoin (BTC) or Ethereum (ETH) through their personal or business crypto wallets.

---

3. Transfer of a virtual asset, whether or not for value

A company engages in this activity if it moves virtual assets from one wallet to another on behalf of clients. For example:

(a) A crypto remittance company that facilitates cross-border transfers using stablecoins (e.g., USDC, USDT) as a cheaper alternative to SWIFT.

(b) A blockchain-based payment processor that enables local businesses to receive crypto payments and automatically settle transactions in another cryptocurrency.

(c) A freelance platform that allows international clients to pay SVG registered freelancers in Bitcoin, with automatic conversion into a preferred virtual asset.

(d) A wallet service provider that offers crypto wallet-to-wallet transfer services.

(e) A merchant or individual who assists users in sending and receiving cryptocurrency on their behalf, often charging a small commission for facilitating the transaction.

---

4. Safekeeping or administering of a virtual asset or instruments enabling control over a virtual asset

This applies when a company provides custody, storage, or security solutions for virtual assets. For example:

(a) A crypto custody provider that stores large amounts of Bitcoin or other cryptocurrency in cold storage for institutional investors.

(b) A multi-signature wallet provider that helps businesses secure their virtual assets by requiring multiple approvals for withdrawals.

(c) A trust company that offers crypto inheritance planning, ensuring that digital assets are securely passed on to beneficiaries.

(d) A blockchain security firm that provides private key management solutions, helping users recover lost or stolen assets.

(e) A local service provider who assists individuals in setting up and managing their crypto wallets securely, ensuring they have access to their funds and recovery mechanisms in place.

(f) A custodial wallet service holding user' private keys and authorizing transactions on their behalf.

(g) A regulated digital asset vault providing multi-signature cold storage solutions to institutional clients.

(h) A platform offering administrative tools (like delayed withdrawal approvals or account freezes) that indicate control over virtual assets.

---

5. Participating in or providing financial services related to the issue or sale of a virtual asset

This occurs when a company assists in launching, promoting, or structuring virtual asset offerings. For example:

(a) A crypto fundraising platform that helps startups raise capital through an Initial Coin Offering (ICO) or Security Token Offering (STO).

(b) A tokenization service that converts real-world assets (e.g., real estate, art, or commodities) into digital tokens for fractional ownership.

(c) A digital asset advisory firm that structures new cryptocurrency projects, providing guidance on token economics and regulatory compliance.

(d) A marketing agency specializing in promoting new crypto projects and token sales to international investors.

(e) A crypto exchange or brokerage that facilitates the listing of new virtual assets for trading.

(f) A local consultant who provides guidance to businesses or individuals on how to invest in new token offerings or how to participate in upcoming crypto projects.

(g) A merchant who assists clients in purchasing new tokens during pre-sales or ICO phases by handling the cryptocurrency conversion process for them.

ANNEX 2- GUIDANCE ON STATUTORY DEPOSITS

1. Statutory Deposits – Acceptable forms of Government Securities

Government securities are financial instruments including **treasury bills, notes and bonds** that are issued by a sovereign and sold to the public. Backed by the full faith and credit of the issuing Government, these instruments are usually considered safe investments.

Treasury Bills are short-term instruments issued with a term of one year or less. They are sold at a discount from face value (par) and do not pay interest before maturity. The difference between the purchase price of the bill and the amount that is paid at maturity (par), or when the bill is sold prior to maturity, is the interest earned on the bill.

Treasury Notes and Bonds bear a stated interest rate, and the owner receives periodic, typically semi-annual income. Treasury notes have a term of more than one year but less than ten. Treasury bonds are long-term instruments issued with a term of more than 10 years.

---

2. Statutory Deposits - Procedural mechanisms for calculating the "25% of the financial obligations to Client's "threshold"

Step 1: Define Financial Obligations to Clients:

The financial obligations to client would include:

- All digital assets being held on behalf of the client
- Any fiat currency being held in bank accounts or payment processors on behalf of the clients
- Pending client withdrawals requests or unsettled trade obligations
- Operating loans made to the VABS by clients
- Any other contractual obligations to deliver or return value to the clients

For entities already existing upon applying for registration under the Act, the best way to ascertain the client's obligation will be to request the internal client ledger that shows client balances. Using a balance sheet may not be the most appropriate, as balance sheets may not often be disaggregated to show the assets belonging to the client only.

Step 2: Identify a Valuation date

It is recommended that this date be the application date. Thus, the ledger should be requested as of the application date.

Step 3: Value the Asset

Ensure the valuation is converted to one (1) single currency (USD).

Step 4: Calculating the total Financial Obligation to clients

Add all the relevant client balances as applicable.

Step 5: Apply the 25% threshold to the total financial obligation to clients

Required statutory deposit = 0.25 x Total financial obligation to clients

NOTE: In the case of a new business applicant, there may be no existing records from which to determine financial obligations to clients. In such instances, the statutory deposit requirement shall default to **one hundred thousand dollars (EC$100,000)**.

---

3. Statutory Deposits - Assessment methodologies for determining the duration of retention post-cessation of operations of Virtual Assets Business ('VAB')

A VAB which has ceased to offer or operate such business in/from SVG must proceed to wind up and dissolve pursuant to the Business Companies Act or the Limited Liability Company Act. The FSA will release the statutory deposit after conducting a review of:

1. The last annual risk management report. This report would have addressed the extent to which a licensee met its risk management requirements imposed by the FSA and the requests therefrom to implement systems to assess and maintain for the nature/level of risks to which it is/might be exposed. The relevant risks are:
2.
   (a) if the VAB has to be wound up will it be done in an orderly manner;
   (b) meeting its obligations: capital and liquidity.

The findings thereof will be reported in the release of statutory deposit memo/recommendation,

see 2 (c) below, for information.

3. Liquidation reports and other documents - The Authority shall release tranches of the statutory deposit to the Liquidator, as deemed appropriate, during the liquidation. These releases are granted upon the request of the Liquidator to the FSA and upon production of the interim liquidation/liquidator reports and all is in order. The FSA shall pay over the proceeds of the statutory deposit balance when the liquidation has concluded and the Liquidator has issued its final report and other dissolution documents and payment for the certificate of dissolution. Partial releases can be done over the course of the Liquidation particularly if sufficient liquid funds have not been recovered and urgent payments have to be made. Such releases will be so approved with the requisite supporting documentation, such as an interim liquidation report and is done at the discretion of the Executive Director.

   If an involuntary liquidation the documents shall be reviewed against the terms of the Court Order (in the case of an involuntary liquidation). The cash balance on the Statutory Deposit account maintained by the FSA should also be assessed.

   Any fees due to the FSA shall be deducted from the total of the statutory deposit principal.

ANNEX 3- GUIDANCE ON SECTION 6(2) OF THE ACT AND REGULATION 3 OF THE REGULATIONS

1. AML/CFT Policies and Procedures

AML/CFT Measures

The AML/CFT policy of an entity functions as a formal document that articulates the VAB's approach to identifying, mitigating, and managing the risks associated with money laundering (ML) and terrorist financing (TF). It offers a clear, comprehensive, and actionable framework for:

- Customer due diligence and onboarding;
- Enhanced due diligence
- Transaction and Ongoing monitoring
- Identification and reporting of suspicious activity
- Sanctions and politically exposed person (PEP) screening;
- Record-keeping and data confidentiality
- Compliance governance and training; and
- Internal audits and control evaluations

The policy should be more than a generic template; it must be tailored to the applicant's business model, size, complexity, and specific Virtual asset services offered. The applicant must implement a framework consistent with the following recommendations and legislative requirements:

- The Financial Action Task Force (FATF) Recommendations
- Proceeds of Crime Act, 2013
- Anti-Money Laundering and Terrorist Financing Regulations, 2014
- Anti-Money Laundering and Terrorist Financing Code 2017
- Financial Services Authorities Act
- Virtual Asset Business Act 2022

Core Components of a Compliant AML/CFT Policy

a. Governance and Oversight:

The policy must:

- Define the responsibilities of the AML/CFT Reporting and Compliance Officer;
- Describe the role of senior management in ensuring AML/CFT compliance
- Explain how AML/CFT responsibilities are embedded across departments;

- Detail escalation procedures and lines of reporting.

b. Risk-Based Approach:

The policy must:

- Explain the methodology used for assessing ML/TF risks;
- Show how customers, products, delivery channels, and geographies are risk-rated;
- Describe how risk scores influence onboarding, monitoring, and review frequency;
- Integrate the latest FATF high-risk country advisories and sanctions regimes.

c. Customer Due Diligence (CDD) and Know Your Customer (KYC):

The policy must:

- Outline procedures for customer identification and verification;
- Outline procedures regarding Beneficial ownership verification;
- Outline the Standards for initial and ongoing CDD;
- Outline the requirements for Enhanced Due Diligence (EDD), particularly for PEPs, high-risk countries, or large/complex transactions;
- Outline steps for refreshing customer data periodically.

d. Transaction Monitoring

The policy must:

- Describe how suspicious transaction patters are flagged;
- Outline red flags related to Virtual assets (e.g., rapid movement between wallets);
- Detail investigation steps and internal escalation paths
- Reporting Suspicious Activity

The policy must include:

- Definitions of suspicious activity;
- Reporting thresholds;
- Internal reporting procedures;
- Timelines for reporting;
- SAR retention and confidentiality protocols

e. Other Policies to be Outlined:

- Record Keeping and Retention policy: (Retention period, documentation format, assess control policies & periodic data integrity checks)
- Sanctions and Pep screening policy
- Staff training and Competency policy (frequency of training and documentation regarding attendance, material and evaluations)
- Internal Controls and Audit policy (internal monitoring frameworks, independent audit scope and frequency, reporting obligations of the internal audit function).

---

2. Data management and protection frameworks

A person who makes an application for registration to offer/operate virtual asset business is required to provide written policies/rules, technologies and procedures for its data management and protection (DMP) framework[4].. The VAB is required, in its handling of data and its protection, to ensure that it:

- Adopts a structured approach so that data integrity, security, and compliance are maintained;
- Effectively manages data throughout its lifecycle, from collection, to storage, usage, and disposal; and
- Protects data from unauthorized access and breaches.

Key elements of a DMP framework which must be addressed when setting rules/procedures follows:

- *Data Governance*: to establish procedures for managing data as a strategic asset and ensuring its accuracy, consistency, retention policies and security.
- *Data Quality*: focuses on maintaining the accuracy, completeness, and reliability of data, often using techniques for data profiling, cleansing, and validation.
- *Data Security:* the implementation of measures to protect data from unauthorized access, use, disclosure, disruption, modification, or destruction.
- *Data Architecture*: defines the structure, organization, and storage of data, including the choice of technologies and tools.
- *Data Analytics:* enables the use of data for decision-making and business insights.
- *Data Privacy*: handling sensitive data responsibly and ethically. Adhering to relevant regulations and standards for data privacy to ensure compliance.

[4] section 6 (2) (h) of the VAB Act

- *Data Integration*: managing data flow between different applications and systems so that disparate data sources and systems are connected and a unified data view is created.
- *Data Lifecycle Management*: the planned processes that will be implemented for managing data throughout its lifecycle, i.e. from creation to its disposal, including data retention, archiving, and deletion.

Therefore, the VAB will be required to outline the following in its rules/policies/procedures data management framework which will address the aforementioned:

- Controls: encryption, access, loss prevention and secure data storage for client information.
- Risk-based controls for the protection of data throughout its life cycle. This includes data loss prevention capabilities and controls for data at rest, data in transit and data in use
- Intrusion detection systems.
- Use of data techniques for profiling, cleansing and validation.
- Use of any technologies and tools.
- Use of data warehousing, ETL processes, and business intelligence tools.
- Applicable data protection regulations and international data security standards of overseas jurisdictions which the VAB must comply with.

---

3. Security access control protocols

Safeguarding digital assets has become a critical priority in an increasingly digital world. With the rise of cryptocurrencies and other digital investments, robust cybersecurity practices are essential to protecting these valuable assets from theft, fraud, and cyber-attacks.

Securing cryptocurrency wallets is fundamental to protecting digital assets from theft and unauthorised access. A robust security strategy begins with using strong, unique passwords and enabling multi-factor authentication (MFA) to add an extra layer of protection. Regularly updating your wallet software ensures you benefit from the latest security patches and features.

For those holding significant amounts of cryptocurrency, using hardware wallets provides enhanced security by storing assets offline, away from online threats. Additionally, it is important to be cautious of phishing attempts and malware. Always back up wallet private keys in a secure location as implementing these measures can significantly reduce the risk of losing valuable digital assets to cyber criminals.

- ***Protecting Cryptocurrency Exchanges***

  Protecting cryptocurrency exchanges is crucial given their role as primary targets for cybercriminals. To ensure the safety of transactions, choosing an exchange that implements strong security measures is essential.

  Therefore, users are encouraged to look for platforms that utilise robust encryption methods, conduct regular security audits, and have secure server infrastructures to protect user data. Implementing multi-factor authentication (MFA) and maintaining complex, unique passwords for accounts are additional steps that enhance security.

  Staying informed about any security breaches or updates from one's exchange can also help you take timely action to protect your assets. By prioritising these security practices, you can safeguard your cryptocurrency transactions and investments from potential threats.

- ***Avoiding Phishing Scams***

  Avoiding phishing scams is essential for safeguarding digital assets from cybercriminals who attempt to steal sensitive information through deceptive tactics. Phishing scams often come in the form of fraudulent emails, messages, or fake websites designed to trick users into revealing personal details or login credentials.

  To protect yourself, always verify the authenticity of any communication claiming to be from financial institutions or cryptocurrency services. Check for secure, legitimate website URLs and avoid clicking on links or downloading attachments from unknown sources.

  Be cautious of unsolicited requests for sensitive information, and use tools like email filters and anti-phishing software to detect potential threats. By staying vigilant and practising careful online behavior, you can effectively reduce the risk of falling victim to phishing scams.

- ***Implementing Network Security Measures***

  Implementing network security measures is essential for protecting digital assets from a wide range of cyber threats. For example, when handling transactions involving cryptocurrencies, it is crucial to ensure that the network is secure against potential breaches.

  Firewalls should be used to prevent unauthorized access and ensure all communications are encrypted through secure protocols such as HTTPS and VPNs.

  Regularly update all software and systems to address vulnerabilities and protect against emerging threats. Employing solid passwords and conducting frequent network audits will help identify and mitigate security risks. By adopting these

comprehensive network security measures, users can effectively safeguard their digital transactions and protect assets from cyber threats.

- ***Conducting Regular Security Audits***

  Regular security audits are critical for maintaining the integrity and safety of digital assets. These audits involve thoroughly reviewing your security infrastructure, identifying vulnerabilities, and assessing the effectiveness of existing protection measures.

  Engaging cybersecurity experts to perform these assessments ensures that potential weaknesses are detected and addressed before malicious actors can exploit them. Regular audits help verify that systems are up-to-date with the latest security patches and standards, and they can also reveal areas where additional safeguards may be needed. By systematically evaluating and strengthening security posture through periodic audits, can enhance defenses and protect valuable digital assets from evolving cyber threats.

---

4. Cybersecurity safeguards

Virtual assets, such as cryptocurrencies, non-fungible tokens (NFTs), and digital tokens, have become integral to the digital economy. However, with the increasing value of these assets, they also attract a wide range of cyber threats, including hacking, phishing, and malware attacks. The protection of these assets requires a proactive, multi-layered approach to cybersecurity. Below are some key guidance and best practices:

A. Private Key Protection

A private key is a cryptographic key that allows the owner to access and control their virtual assets. Loss of the private key or exposure to unauthorized parties can result in theft or loss of assets.

- **Private Keys = Security**: Private keys are essentially the keys to your virtual assets. If someone else gains access to your private key, they can access your digital assets. Therefore, safeguarding private keys is paramount.
- **Hardware Wallets**: Use hardware wallets (e.g., Ledger, Trezor) to store private keys offline. These wallets are immune to online threats such as hacking or phishing attacks.
- **Encryption**: Always encrypt private keys, especially when storing them on a device. Consider using multi-signature wallets where multiple parties must sign off on a transaction.

- **Backups**: Backup private keys securely, preferably using encrypted offline storage or paper wallets. Never store backups in cloud services or online.

B. Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) adds an additional layer of security by requiring two or more forms of verification (something you know, something you have, or something you are).

- **MFA Everywhere**: Use multi-factor authentication (MFA) for all accounts related to virtual assets (exchanges, wallets, email). This typically involves something you know (password) and something you have (an authentication app, phone, or hardware token).
- **Avoid SMS-Based MFA**: SMS-based MFA is vulnerable to SIM swapping attacks. Use authenticator apps (e.g., Google Authenticator, Authy) or hardware tokens (e.g., YubiKey) for stronger security.

C. Cold Storage vs. Hot Storage

Cold storage refers to storing virtual assets offline, making them less susceptible to cyberattacks.

- **Cold Storage**: Store the majority of your digital assets in cold storage (offline wallets), which are not connected to the internet. This minimizes exposure to cyber threats.

Hot storage refers to wallets connected to the internet. These are more vulnerable to cyber threats but are necessary for active trading or transactions.

- **Hot Storage**: Only keep the small amount of virtual assets needed for active trading in hot wallets (online wallets). Keep the hot wallet secured with strong encryption and MFA.

D. Phishing and Social Engineering Protection

Phishing attacks trick users into revealing sensitive information like passwords, private keys, or MFA codes.

- **Education**: Be cautious of phishing attacks where attackers impersonate exchanges or wallet providers. Never click on links or open attachments from untrusted sources.
- **Verify URLs**: Always ensure you are on the correct website (check the URL) before entering sensitive information like private keys, passwords, or MFA codes.

- **Social Media Caution**: Be wary of offers that seem too good to be true, such as fake giveaways or investment schemes, especially on social media platforms.

E. Secure Networks

- **VPN (Virtual Private Network)**: Use a trusted VPN when accessing your virtual assets, particularly when connecting to public or untrusted networks.
- **Avoid Public Wi-Fi**: Never use public Wi-Fi for accessing cryptocurrency exchanges or wallets. If you must, use a VPN to encrypt your connection.
- **Use Trusted Devices**: Avoid accessing your virtual assets from devices you do not fully control or trust. This includes public computers, shared devices, or unverified devices.

F. Regular Software Updates

- **Patch Vulnerabilities**: Always keep your wallet software, antivirus, and operating system up-to-date. Software updates often fix security vulnerabilities that hackers could exploit.
- **Use Reputable Wallets**: Choose wallets and exchanges that have a track record of secure practices and that release regular updates to their software.

G. Secure Exchange Practices

- **Use Reputable Exchanges**: Only use well-known and regulated cryptocurrency exchanges for buying, selling, or trading virtual assets.
- **Withdrawal Limits and Whitelisting**: Set up withdrawal limits and add trusted withdrawal addresses (whitelisting). This prevents an attacker from transferring assets to an unknown address even if they gain access to your account.
- **Withdrawal Notifications**: Set up email or SMS notifications for any withdrawal activity from your account.

H. Asset Recovery Plans

- **Contingency Plans**: Have a plan for recovering access to your virtual assets in case of loss or theft. This includes securely storing backup phrases, hardware wallet recovery keys, and having trusted individuals (e.g., family members) who can assist in recovery.
- **Inheritance Plans**: Consider creating an inheritance plan for your virtual assets, as crypto assets may not be easily transferred after death without proper instructions.

I. Monitoring and Alerts

- **Real-Time Monitoring**: Use portfolio monitoring tools that alert you about suspicious activity or changes in your asset value.
- **Security Alerts**: Set up alerts for transactions or withdrawals on your exchange or wallet. These alerts can help you detect unauthorized access early.

J. Legal and Regulatory Compliance

- **Know Your Rights**: Stay informed about the legal protections available for your virtual assets based on your jurisdiction.
- **Insurance**: Some services and platforms offer insurance for digital assets. Research whether these services are available and what they cover.
- **Regulated Exchanges**: Prefer exchanges that comply with relevant regulations and offer consumer protections.

K. Decentralized Finance (DeFi) Risks

- **Smart Contract Vulnerabilities**: DeFi protocols rely on smart contracts, which can have bugs or vulnerabilities. Conduct thorough research before interacting with DeFi platforms.
- **Liquidity Risks**: Be aware that DeFi platforms may involve risks such as liquidity problems, rug pulls, or unverified token contracts.
- **Audits**: Choose DeFi protocols that have been audited by reputable cybersecurity firms.

L. Secure Development (for Developers)

- **Secure Smart Contract Code**: If you are developing smart contracts, ensure the code is audited and free of vulnerabilities.
- **Best Practices for Code**: Follow industry best practices in secure coding, such as avoiding hard-coded keys, using safe libraries, and testing your contracts rigorously.
- **DeFi Security Tools**: Use advanced security tools such as static analysis tools, fuzz testing, and formal verification to check for vulnerabilities in smart contract code.

The chart below is intended to be used as a reference tool to guide policy development, risk assessments, and audit preparation. It consolidates essential controls under each relevant area, ensuring that both technical and governance-related aspects of cybersecurity are addressed in a holistic manner.

Control Area	Key Measures
Private Key Security	Store keys offline (cold wallets), use multi-signature wallets, encrypt backups, geographically separate.
Access Control	Enforce MFA (no SMS), implement RBAC, conduct periodic access reviews, maintain audit logs.
Network Security	Deploy firewalls, IDS/IPS, endpoint security, VPN, encrypted communications, patch management.
Phishing Defense	Staff training, anti-phishing tools, and protocols.
Monitoring & Response	Real-time alerts, documented incident response plan, escalation procedures, regulatory reporting.
Security Audits	Regular internal and external audits, penetration testing, vulnerability assessments.
Business Continuity	Disaster recovery plans, regular backups, crypto inheritance protocols.
Regulatory Compliance	Alignment with Virtual Asset Business Act, AML/CFT, data protection laws, ISO 27001, NIST CSF, FATF

5. Risk assessment documentation

The risk assessment is a critical tool for identifying, evaluating and mitigating risks related to money laundering (ML) and terrorist financing (TF), and other financial crimes. Below are the critical areas which must be outlined in this document.

i. Introduction and Objectives:

- Clearly define the purpose and scope of the risk assessment
- Reference applicable regulatory obligations under the Virtual Asset Business legislation
- State the overall risk management objectives of the entity.

ii. ***Risk Identification Framework****:*

The document should identify and describe the various categories of risk considered, including but not limited to:

- Customer risk
- Product/ service risk
- Delivery channel risk
- Geographic risk

Third party risk should also be considered in context of reliance on custodians or technology providers.

iii. ***Risk Evaluation and Scoring****:*

The document should include the following:

- The assessment should clearly define the risk scoring methodology (quantitative and/or qualitative)
- There should be criteria and thresholds established for categorizing risk (e.g low, medium, high)
- The rationale for assigning risk ratings to different business components.
- Description of any tool or models used for risk quantification

iv. ***Risk Mitigation Measures:***

The risk assessment document must outline the following:

- Specific controls in place to manage each identified risk
- Preventative and detective measures (e.g., KYC procedures, transaction monitoring, SAR filing protocols).
- Use of enhanced due diligence for high-risk customers or activities
- Assignment of responsibilities for control implementation and monitoring.

v. ***Residual Risk Assessment:***

The risk assessment document should demonstrate clearly:

- Analysis of residual risks after the application of mitigating controls
- Justification of entity's risk tolerance and residual exposure levels
- Linkage to the institution's defined risk appetite framework.

vi. ***Review and Update Procedures****:*

The risk assessment should describe:

- Frequency of risk assessment reviews (e.g., annually or upon material changes)
- Triggers for interim reviews (e.g., new products, emerging threats, regulatory updates)
- Processes for tracking changes and maintaining version control.

vii. Governance and Oversight:

The risk assessment must include evidence of governance such as:

- Board or senior management approval of the assessment
- Oversight mechanisms to ensure accountability for risk management

COMMENCEMENT

These Guidelines shall come into effect this 18th day of November 2025

Issued by:

Financial Services Authority
P.O. Box 356
Kingstown
St. Vincent & the Grenadines
Tel (784) 456-2577
Fax (784) 457-2568
Email: info@svgfsa.com