# Virtual Asset Services Providers (VASP) Act No. 3 of 2025

# Agenda

o**INTRODUCTION**

oVASP License Classes

oVASP Fees

oApplication Requirements

oApplication Process

oInitial Token Offering (ITO)

oFintech Sandbox Utility

o**-TEA BREAK-**

oManagers and Directors

oAML/KYC and VASP Risk Management

oCustodian

oExternal Audit

oRecord Keeping

oSecurity Breaches

o**CONCLUSION / LUNCH**

# Introduction

# Purpose of the Act

To provide for:

o       Establishment of virtual assets, virtual tokens and virtual assets service providers.

o       Licensing of Virtual Asset Service Providers (VASP), Initial Token Offering (ITO) and Fintech Sandbox.

# Stable coins or CBDC not covered

- Virtual Assets vs Stable Coins
  - The main difference between virtual assets and stable coins is that stable coins are backed by fiat currency while virtual assets are not
  - As a result, virtual assets tend to fluctuate a lot and are more volatile while stable coins are more stable

*Note: This act does not cater for stable coins or Central Bank Digital Currency (CBDC)*

# Guidelines and Application Forms

- Since the Act has been gazette, the Commission has issued 3 guidelines and 4 different application forms that can be used for application purposes.

- These can be found on the link below:

https://www.vfsc.vu/virtual-asset-service-provider/

# VASP License Classes

| License Class | Activity |
| --- | --- |
| Class D license | Authorize the exchange between virtual assets and fiat currencies or the exchange between one or more forms of virtual assets |
| Class D.1 license | Authorize the transfer of virtual assets |
| Class D.2 license | Authorize the safekeeping of virtual assets or enabling control over virtual assets |
| Class D.3 license | Authorize the participation in and provision of financial businesses related to both or either an issuer's offer and sale of virtual assets |
| Class D.4 license | Authorize a bank to operate the exchange between virtual assets and fiat currencies and the safekeeping of virtual assets or enabling control over virtual assets. |

# VASP Fees

Per section 66 of the VASP Act, all application and licensing fees are as tabled below:

| Service | Fee |
|---|---|
| Manager's Application Fee | VT 200,000* |
| CTO's Application Fee | VT 200,000* |
| Director's Application Fee | VT 200,000* |
| VASP Class D Application fee | VT 20,000,000 |
| VASP Class D License fee | VT 100,000,000 |
| VASP Class D.1 Application fee | VT 20,000,000 |
| VASP Class D.1 License Fee | VT 100,000,000 |
| VASP Class D.2 Application fee | VT 20,000,000 |
| VASP Class D.2 License Fee | VT 100,000,000 |
| VASP Class D.3 Application fee | VT 20,000,000 |
| VASP Class D.3 License Fee | VT 100,000,000 |
| VASP Class D.4 Application fee | VT 20,000,000 |
| VASP Class D.4 License Fee | VT 50,000,000 |
| Fintech sandbox application Fee | VT 200,000 |

*Only applies to _any changes/ replacement_ to Managers, CTO's and Directors. A fee is **NOT** charged on the initial Application.

# Annual Fees

| Service | Fee |
| --- | --- |
| VASP Class D License fee | VT 50,000,000 |
| VASP Class D.1 License fee | VT 50,000,000 |
| VASP Class D.2 License fee | VT 50,000,000 |
| VASP Class D.3 License fee | VT 50,000,000 |
| VASP Class D.4 License fee | VT 25,000,000 |
| Fintech Sandbox License fee | VT 50,000,000 |

# Application Requirements

# Requirement of Applications

- Application in the prescribed form and fees.

- State the class or classes of VASP.

- State any third party as part of the application.

- Proposal in the Statement of the services.

- Proof of physical presence.

- Key persons.

- Source of funds details.

- Managers and Directors applications.

- Commission may require the applicant to provide additional information for assessing the application.

# Assessment of the Application

- ✓ Financial Information and documents must viable.
- ✓ Officers, registered agent, and person acting on instruction are fit and proper.
- ✓ Business is financially viable.
- ✓ Services provided by the applicant will not bring Vanuatu into disrepute as an international financial center.
- ✓ All key persons are fit and proper person.
- ✓ Source of funds used to pay capital of the applicant is acceptable.
- ✓ Information supplied by the applicant is complete, not false or misleading.
- ✓ Prescribed fees are paid.
- ✓ Additional information and documents are provided within the specified time.
- ✓ The applicant is compliant with the requirements of the Act, Regulations, and Guidelines.

# Application Process

# Application Process

- Very similar to FDLs application;

- All VASP License applications must come through an active Agent

- Minimum stated unimpaired capital of not less than VT 200,000,000 or such higher amount as the VFSC may determine. (Can be held externally in a recognized Financial Institution and certified by an external auditor)

An applicant shall –

➢ Ensure that its governance structure provides effective oversight of its activities, taking into consideration the nature, scale and complexity of its business;

➢ Establish adequate internal controls and adopt strategies, policies, processes and procedures in accordance with principles of sound corporate governance and risk management;

➢ Maintain its registered office and place of business in Vanuatu; and

➢ Have a board of directors, at least one of whom shall be resident in Vanuatu;

➢ Its CTO must reside in Vanuatu;

➢ Physical presence in Vanuatu.

# Initial Token Offering (ITO)

# Requirements for issuing Initial Token Offering (ITO)

ITO's can only operate if they acquire a license under the Act.

Only Companies can apply for an ITO license.

A person operating without a license is liable to the following fines upon conviction:
- VT 25 Millions and 15 years imprisonment for individual;
- VT 250 Million for body corporate.

# Application for Initial Token Offering (ITO)

The application for an ITO must include the following:

- Complete the prescribed application forms.

- Paid prescribed fees.

- Certificate of incorporation.

- Proof of physical presence in Vanuatu.

- White paper with a written legal opinion from an expert lawyer in Virtual Assets.

- An approval letter, in respect to the initial token offering issued by a VASP licensee within or outside of Vanuatu.

- Policies and measures adopted to meet the requirement of AML/CTF Act.

- Disclosure of UBO and KYC.

- Proof of 2 years experiences in the business of ITO.

# Initial Token Offering License Conditions

The Commission can impose conditions and can also amend and rectify the conditions based on the operation state of the ITO.

# Fintech Sandbox Utility

# Fintech Sandbox Utility

- Company intending to carry on an Innovative Fintech Sandbox Utility must apply to the Commission for approval.

- Company must have at least 1 years experience in Fintech Sandbox utility.

- A Company intending to deal in Fintech Sandbox Utility may apply for any of the following categories:
  - Virtual assets broker dealer,
  - Virtual asset wallets services,
  - Virtual asset custodian,
  - Virtual asset advisory services,
  - Virtual asset exchange and Product that fall under licences A, B, C of the FDL Act.

- An approval for a Fintech Sandbox business activity is for a period of 12 months and may be renewed.

# TEA BREAK

# Manager, Director & Chief Technology Officer (CTO)

# Managers and Directors

Requirement for becoming a Manager / Director in a VASPs and Initial Token Offering(ITO):

- Both Directors and Managers must be fit and proper according to the Act and Guideline;

- Citizen and non citizen are eligible to apply for both directors and managers except that non citizen must reside in Vanuatu for not less than 12 consecutives months after being approved as a manager or director.

- Manager must have at least 5 year experience in the work of VASP or ITO

- Director's must have at least 2 years experience in the work of VASP or ITO.

- Both Directors and Managers must have an office in Vanuatu.

# Chief Technology Officer (CTO)

- A CTO is required to continuously reside in Vanuatu for a period of at least 12 consecutive months.

- The individual must have qualifications in engineering, Computer Science or any related field with at least 1 year experience in the work of a virtual asset service provider or management

# AML/KYC & VASP Risk Management

# AML & KYC Requirements

As part of its application documentation:

❑ the applicant will be required to submit a detailed report containing an in-depth assessment of the potential money laundering and terrorist financing ("ML/TF") risks posed by its operations as well as the measures, systems, controls and protocols which will be established in relation to those ML/TF risks.

❑ Once licensed, prior to starting its operations, the licensee will be required to have those ML/TF systems and controls in place.

❑ As part of its systems and controls to prevent ML/TF, the applicant must have in place procedures to conduct CDD and KYC as well as to ascertain the source of funds/wealth of potential clients prior to on-boarding.

*Note: VFSC has completed a VASP Risk Assessment which will be published and made available to the public as part of the National Risk Assessment.*

# Operational Risk Management

Management of operational risks

❑The applicant's procedures must include a comprehensively documented operational risk management programme (ORMP) which shall include all current industry risks and be audited on an on-going basis to cater for emerging risks to its business. This ORMP, to be applied in the operations of the applicant and communicated to all relevant personnel, will need to include, at a minimum:

➤ Strategies developed to identify, assess, monitor and control/mitigate operational risks;

➤Policies and protocols relating to operational risk management and controls;

➤Methodology to assess operational risks; and

➤Operational risk reporting system.

# Custodian

# Custodian License Requirement

☐ Custodian licence under D.2 License

In assessing the capacity of an entity to provide custody services for Virtual Assets, the approach contemplated by the VFSC will focus on three core areas for this activity, namely:

1. Operational and Governance Protocols – The policies and protocols as well as operational risk management, including fraud prevention, in relation to the custody of Virtual Assets.

2. Safekeeping of Virtual Assets – The generation and securing of seeds and keys as well as management of addresses and wallets relating to Virtual Assets. This area also extends to recovery processes regarding seeds and keys which have either been corrupted or otherwise compromised.

3. Transaction Management – The procedures for the facilitation of incoming and outgoing transactions in relation to a Virtual Asset being held in custody to ensure that appropriate Know Your Client ("KYC") and Customer Due Diligence ("CDD") measures are applied prior to any transactions being authorised.

# Disclosure to Client by the Custodian

The VFSC considers that the protocols of the applicant must also cater for the following disclosures:

❑ Each client to be provided with an original of the signed agreement regarding the custody of his Virtual Assets at the time of on-boarding;

❑ Thereafter, client to be informed of any action which is likely to impact on the signed agreement; and

❑ Any occurrence which may have an incidence on the Virtual Assets belonging to the client being held in custody;

# Custody Processes and System Testing

❑ Once a custodian as been licensed by the VFSC, the custody processes and systems in place must be tested on a scheduled recurrent basis with evidence of such tests and findings thereof being appropriately documented. Such findings must be made available to the VFSC for inspection, or upon request.

❑The schedule for system testing must be included in its protocols to be submitted to the VFSC at the time of application.

❑The recurrent testing schedule must mandatorily take into consideration procedural risks as well as high impact financial risks and may also extend to:

➢Penetration testing and vulnerability scans;

➢Wallet integrity audits;

➢Key and seed generation procedures;

➢Completed transaction audit to ensure compliance with protocols;

➢Suspicious transaction handling;

➢Migration of storage devices (cold to hot storage and vice versa); and

➢Proof of reserves audits.

# External Audit

# External Audit of Policies and Procedures

- The applicant must have in place appropriate arrangements for its policies and procedures to be externally audited.

- The external audit findings must be used to address any shortcomings identified.

- Records of the audit findings along with documentation of any remedial actions implemented must be kept and made available for inspection or provided to VFSC upon request.

- The VFSC recommends that the first external audit be conducted within the first year of operation and thereafter on a recurrent basis, in line with industry best standards and practices.

# Record Keeping

# Record Keeping

- The systems of the applicant must have properly documented procedures relating to record keeping on its clients, including their respective identity as well as information on the Virtual Assets kept under custody, including detailed transactional information.

- Such records must be in line with the appropriate statutory requirements and must be available for inspection upon request by the VFSC.

- Transactional information to be maintained on record to include:

  ➢ Transaction time stamp;

  ➢ Transaction type;

  ➢ KYC/CDD on parties to the transaction;

  ➢ Relevant signatories and transaction approval/rejection evidence;

  ➢ Account balances; and

  ➢ Transaction value.

- The applicant may consider keeping its records and data using blockchain technology for immutability and must be kept for 7 years.

# Security Breaches

# Security Breaches

The protocols of the applicant will need to clearly spell out the procedures, which are to be periodically audited, to be actioned in the event, or suspicion thereof, that a security breach has occurred including:

- hacking,

- attack,

- theft or any situation whereby a Virtual Asset being kept in custody has been compromised.

- The systems of the applicant will have to incorporate appropriate actions specifically designed to protect the Virtual Assets being held in custody in the event of security breaches.

- The policies of the applicant will have to extend to duly notifying the relevant client of the security incident.

# THE END

Tankio tumas


Eni Kwesten?