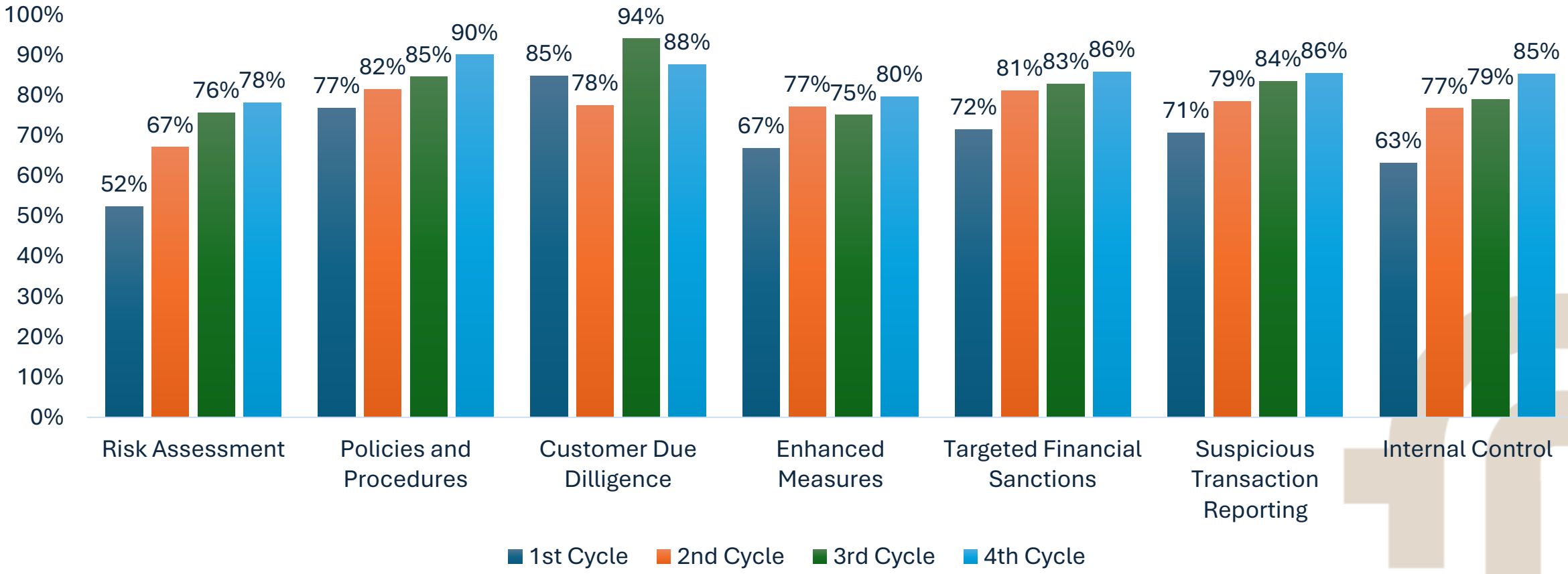
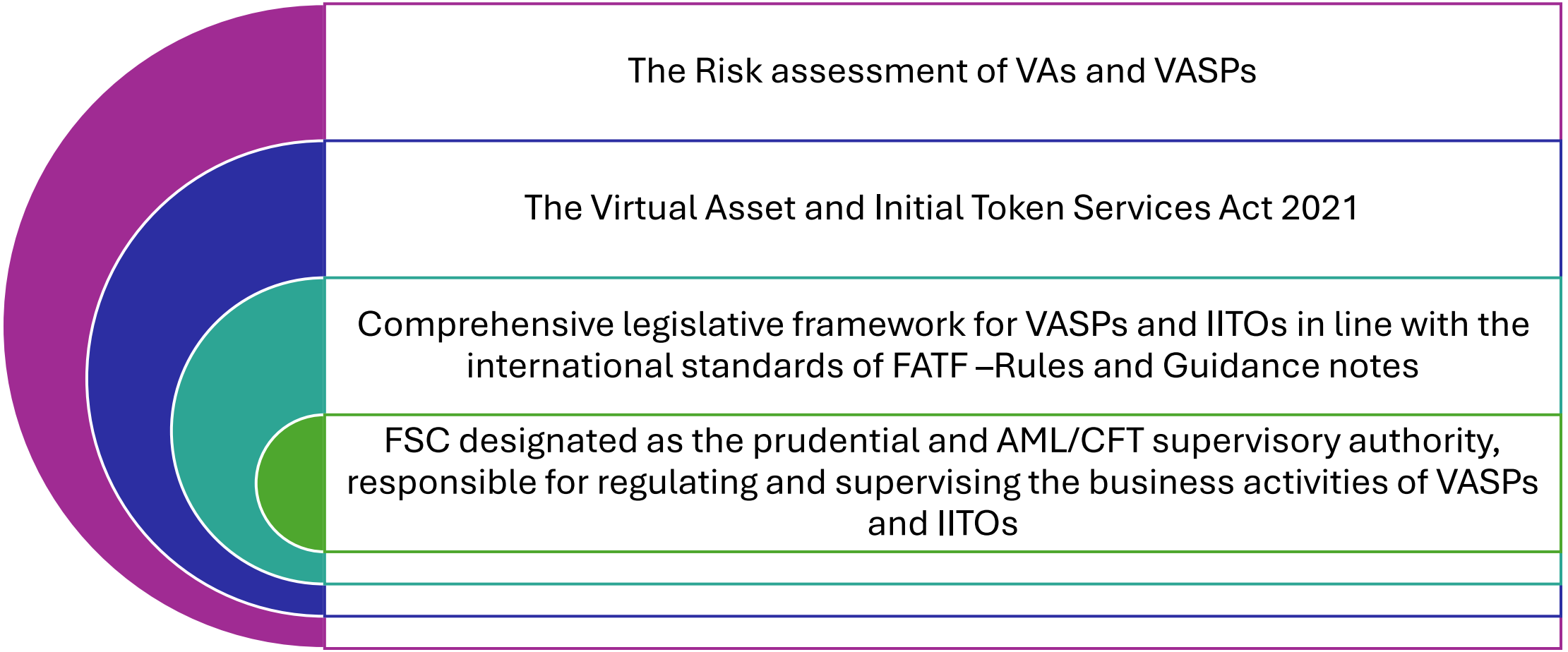
FSC's RBS AML/CFT Supervision Cycles

Precycle 2020	Cycle 2020-2021	Cycle 2021-2022	Cycle 2022-2023	Cycle 2023-2024
• 2221 Offsite Monitoring Questionnaires (OMQs)	• 1909 OMQs • 364 Onsite Inspections • 407 Policy Reviews	• 1895 OMQs • 347 Onsite Inspections • 650 Offsite Reviews	• 1750 OMQs • 335 Onsite Inspections • 612 Offsite Reviews	• 2479 OMQs • 334 Onsite Inspections • 431 Offsite Reviews

FSC's RBS AML/CFT – Compliance Rate



FATF Recommendation 15- Mauritius



Crypto Markets Trends: Recent development

- The crypto landscape has evolved extensively, with criminals discovering new ways to leverage blockchain technology for nefarious purposes. In 2023 alone, illicit crypto addresses received at least $24.2 billion.
- Crypto scamming and hacking revenue both fell significantly in 2023, with total illicit revenue for each down 29.2% and 54.3% respectively.
- In total, darknet markets and fraud shops received $1.7 billion last year which is a rebound from 2022.
- Sanctioned entities and jurisdictions together accounted for a combined $14.9 billion worth of transaction volume in 2023, which represents 61.5% of all illicit transaction volume .
- In 2023, illicit addresses sent $22.2 billion worth of cryptocurrency to services.
- In 2023, deposit addresses received over $1 million in illicit cryptocurrency, for a total of $6.7 billion which accounts for just 46% of all illicit value received by exchanges for the year.
- Through 2021, Bitcoin led the cryptocurrency of choice among cybercriminals, However, this has changed over the last two years, with stablecoins now accounting for the majority of all illicit transaction volume.

RISK ASSESSMENT OF VAs AND VASPs

Mauritius concluded its National Risk Assessment (NRA) with respect to the VA sector in November 2021.
At the time of the assessment, the overall ML/TF residual risk associated to VAs/VASPs was "**Very High**".

Vulnerability	Threat	Residual
High to Very High	**Medium to High**	**Very High**
Nature and complexity Country risks Customer Types Product and Services Operational features	Nature and profile of VAs Sources of funding Accessibility to criminals	The overall ML/TF residual risk associated to VAs/VASPs after the consideration of the mitigating measures

RISK ASSESSMENT OF VAs AND VASPs- Overall ML/TF Risk

VASPs	Types of Services	Sub-type	Threat Rating	Inherent Vulnerability Rating	Total Risk Rating	Residual Risk Rating
VIRTUAL ASSET WALLET PROVIDERS	Custodial Services	Hot Wallet	High	High	High	High
	Non-Custodial Services	Cold Wallet	High	Very High	Very High	Very High
VIRTUAL ASSET EXCHANGES	Transfer Services	P2P	High	Very High	Very High	Very High
		P2B	Medium	High	High	High
	Conversion Services	Fiat-to-Virtual	Medium	Very High	Very High	Very High
		Virtual-to-Fiat	High	Very High	Very High	Very High
		Virtual-to-Virtual	High	Very High	Very High	Very High
VIRTUAL ASSET BROKING	Payment Gateway	Merchants	High	Very High	Very High	Very High
VIRTUAL ASSET MANAGEMENT PROVIDERS	Fund Management		Medium	High	Medium	Medium
	Compliance, Audit & Risk Management		Low	Low	Low	Low
VIRTUAL ASSET INVESTMENT PROVIDERS	Trading Platforms	Platform Operators	Medium	High	Medium	Medium
		Investment into VA-related commercial activities	Medium	Medium	Medium	Medium

FATF Recommendation 15- Mauritius

In September 2022, the technical compliance re-rating of Mauritius on the Recommendation 15 was upgraded to “Largely Compliant” on the basis of the progress made by Mauritius in addressing the underlying deficiencies.

With this technical compliance upgrade, Mauritius is now “Compliant” or “Largely Compliant” with all the 40 FATF Recommendations.

Legislative Framework

The Virtual Asset Initial Taken Offering Services Act 2021 ("VAITOS ACT") 2021, which came into force on 7 February 2022, provides a comprehensive legislative framework for VASPs and IITOs in line with the international standards of FATF with respect to managing, mitigating and preventing any ML/TF risks.

The VAITOS Act 2021 designates the FSC as the prudential and AML/CFT supervisory authority, responsible for regulating and supervising the business activities of VASPs and IITOs respectively.

Any person carrying out the business activities of a VASP and IITO, in or from Mauritius, shall hold a licence or registration, as appropriate, issued by the FSC.

Legislative Framework

The FSC has issued the AML/CFT Guidance Notes for Virtual Asset Service Providers & Issuers of Initial Token Offerings on the 28 February 2022.

It is established to

- Provide an outlook on the significance of ML/TF risks associated with VA activities and

- Guide VASPs and IITOs with an understanding of their specific AML/CFT compliance obligations under the VAITOS Act 2021.

The Guidance Notes depicts the salient ML/TF red flag indicators which are associated with VAs. This will enable regulated entities under the VAITOS Act 2021 to better identify and prevent the ML/TF risks linked with their business activities and also, to set up adequate controls to mitigate those risks.

Financial Services Commission MAURITIUS

AML/CFT Guidance Notes for VASPs

The FSC has issued the AML/CFT Guidance Notes for Virtual Asset Service Providers & Issuers of Initial Token Offerings on the 28 February 2022.
It is established to:

(1) Provide an outlook on the significance of ML/TF risks associated with VA activities.

The Guidance Notes depicts the salient ML/TF red flag indicators which are associated with VAs.

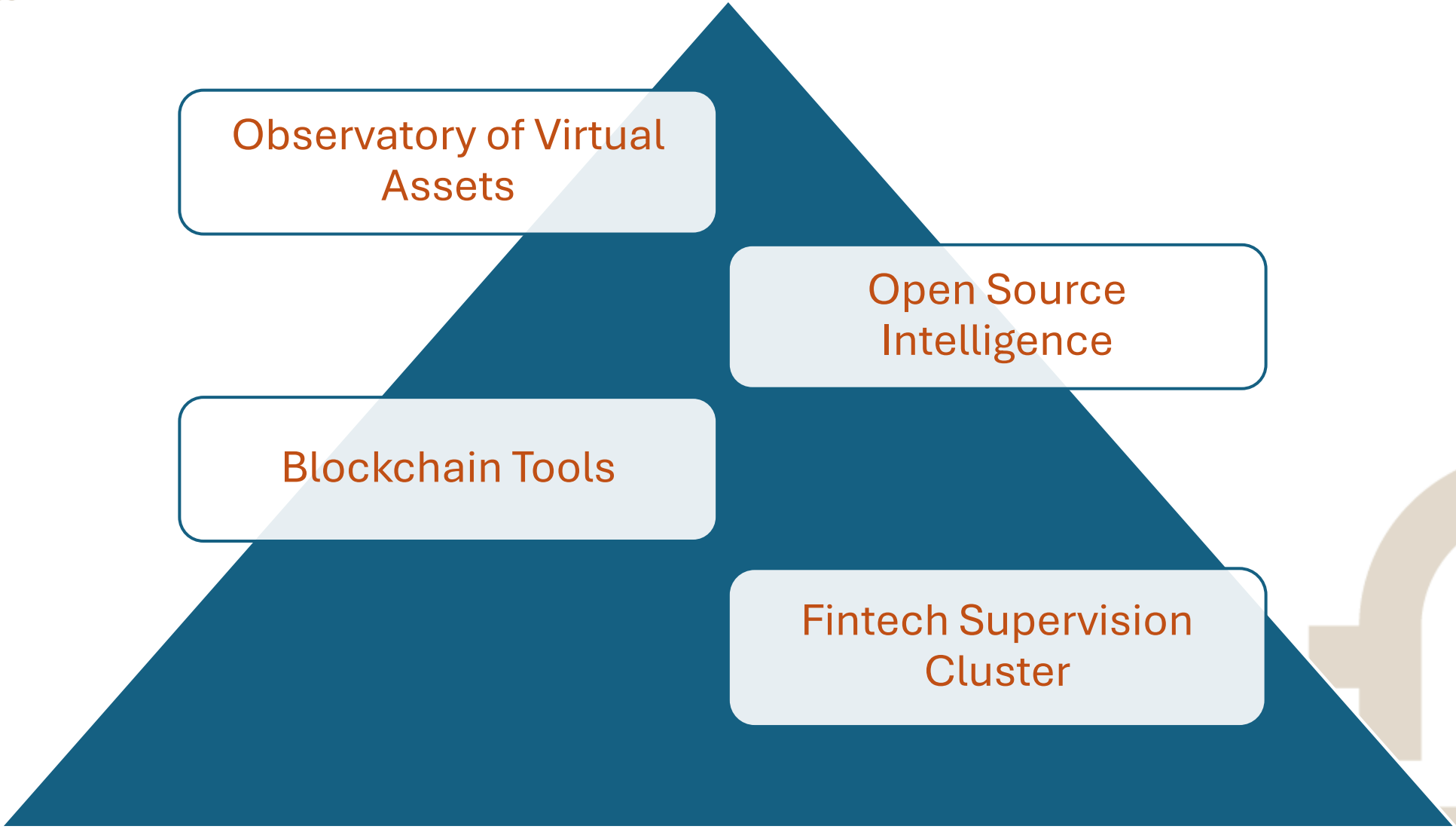
This will enable regulated entities under the VAITOS Act 2021 to better identify and prevent the ML/TF risks linked with their business activities and set up adequate controls.

(2) Guide VASPs and IITOs with an understanding of their specific AML/CFT compliance obligations under the VAITOS Act 2021.

Key AML/CFT compliance obligations to be observed by VASPs and IITOs once/after being licensed or registered, as appropriate, under the VAITOS Act 2021.
They must also comply with the FSC's AML/CFT Handbook.

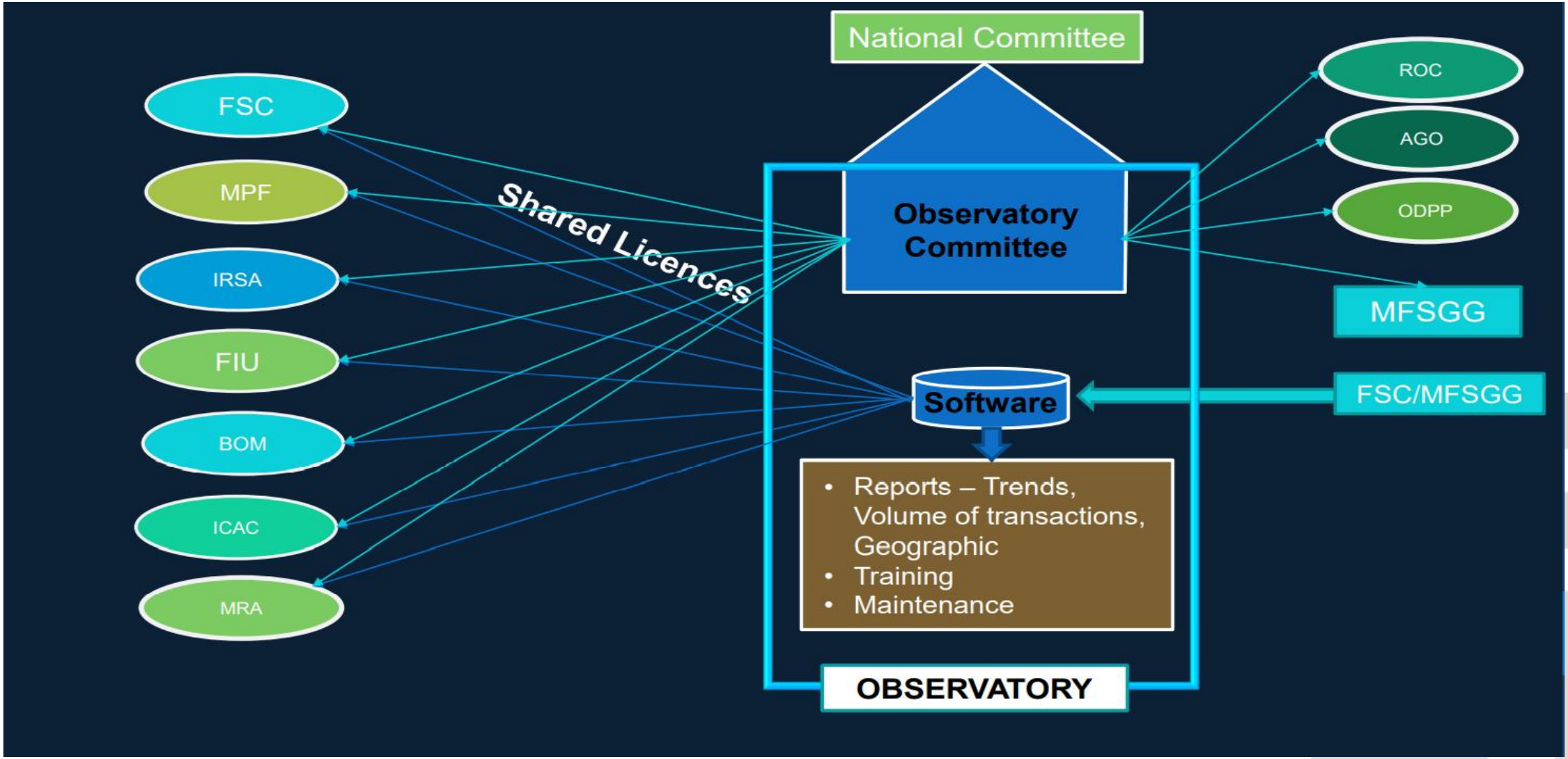
Financial Services Commission MAURITIUS

Supervisory Tools



Financial Services Commission MAURITIUS

Observatory of Virtual Assets



Observatory of Virtual Assets Activities

- **Objectives:**
- ❑ Identify trends and patterns of VA transactions/activities;
-
- ❑ Track and detect unlicensed VASPs;
- ❑ Detect and monitor illegal VA transactions;
- ❑ Share intelligence with other relevant authorities; and
- ❑ Make recommendations on policies, rules and guidelines

Financial Services Commission MAURITIUS

AML/CFT Compliance Obligations

CDD

- VASP and IITOs should maintain accurate and up-to-date customer information. This would include verification of beneficial owners, where applicable, and scrutinising their source of funds and wealth.

EDD

- VASPs and IITOs are required to implement internal controls and other procedures to combat ML/TF, including EDD procedures with respect to high-risk persons, business relations and transactions and persons established in jurisdictions that do not have adequate systems in place to combat ML/TF

Travel Rule

- VASPs and IITOs have the obligation to obtain, hold, and transmit required and accurate originator and beneficiary information, as the case may be, immediately and securely, when conducting any virtual asset transfers

Financial Services Commission MAURITIUS

AML/CFT Compliance Obligations

Transaction Monitoring and Suspicious Transaction Reporting (STR)

- Where a VASP or IITO identifies any suspicious activity or has reasonable ground to suspect that a transaction is suspicious in the course of a business relationship or occasional transaction, it should :
  - obtain EDD,
  - make an internal disclosure and
  - The MLRO should then assess whether a STR needs to be made to the FIU

Risk Based Approach

- VASPs and IITOs are required to identify areas where their products/services could be exposed to ML/TF risks
- The Application of RBA provides a strategy for VASPs and IITOs to manage potential risks by enabling them to subject customers to proportionate controls or oversight.

Occasional Transactions

- In respect to an occasional transaction in amount equal to or above USD 1000 or equivalent, VASPs are required to:
- apply CDD measures
- Record the name of originator and the beneficiary; and the Virtual Asset Wallet Address for each or a unique transaction reference number.

Travel Rules – Recommendation 16

- The Virtual Asset and Initial Token Offerings Services (Travel) Rules 2022 in line with the FATF Recommendation 16, ensures to prevent terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs.

- The Rules aim to ensure that basic information on the originator and beneficiary of wire transfers is immediately available to:

  - intermediary and beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant UNSCR;

  - Detect suspicious activities and the true origin of incoming transmittals; and

  - Assist law enforcement/regulatory bodies in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets.

Red Flag Indicators

Anonymity

- Abnormal volume of VAs cashed out at exchanges from P2P platform-associated wallets with no logical business explanation.
- Receiving funds from or sending funds to VASPs and IITOs with weak or non-existent CDD or Know Your Customer ("KYC") requirements.
- The use of decentralised/un-hosted, hardware or paper wallets to transport VAs across borders.

Transactions

- Structuring of VA transactions (eg exchange of transfer) in small amounts, or in amounts under record keeping or reporting thresholds
- Making multiple high-value transactions – in short succession, such as within a 24-hour period, in a staggered and regular pattern, with no further transactions recorded during a long period afterwards.

Transaction Patterns

- Conducting a large initial deposit to open a new relationship with a VASP, while the amount funded is inconsistent with the customer profile
- A new user attempts to trade the entire balance of VAs or withdraws the VAs and attempts to send the entire balance off the platform.
- Making frequent transfers of large amounts in a certain period of to the same VA account or from same address

Red Flag Indicators (cont'd)

Senders or Recipients

- Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs.
- Incomplete or insufficient KYC information, or a customer declines requests for KYC documents.
- Providing inaccurate information about transaction, or the relationship with counterparty.

Source of wealth or fund

- Transacting with VA addresses that are connected to know fraud, extortion or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites.
- Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an ITO

Geography

- Criminals can potentially exploit the gaps in AML/CFT regimes which are applicable to the VA sector, by moving their illicit funds to VASPs or IITOs domiciled or operated in jurisdictions with non-existent or minimal AML/CFT regulations.
- These jurisdictions may not have a licensing/registration regime, or have not extended STR requirements to cover VA activities, or may not have introduced the full spectrum of preventive measures.

Conclusion Remarks

▪ All entities conducting VA/VASP related activities should be registered and licenced as VASP by the FSC and comply with FIAMLA, FIAMLR, UNSA and AML/CFT Guidance;

▪ Supervised institutions should also implement risk management systems proportionate to the scale and complexity of VA related activities, conduct internal risk assessments, give staff training relevant to VA/VASP sector, and have the appropriate tools and processes to monitor VA transactions and identify their originators and beneficiaries;

▪ As VAs are highly volatile and speculative assets, financial institutions should help customers and stakeholders towards avoiding excessive exposure to VA/VASP risks that might jeopardise their financial wellbeing. It is therefore necessary for financial institutions to increase customers' and investors' understanding of VAs and their education should be prioritised as a key strategy;

- Capacity Building and trainings

▪ Enhanced cooperation protocols and MOUs for exchanging VA/VASP related information