Implementing AML/CFT Programmes

A Guidance Note for non-bank financial institutions conducting virtual assets business

Issued March 10, 2025

NBFIRA

Non-Bank Financial Institutions Regulatory Authority

Disclaimer

This Guidance Note is authored by the NBFIRA in line with section 49(1)(c) of the Financial Intelligence Act, 2022 as amended in 2025 and Regulations, 2022 ("FI Legislation"), and section 4(1)(c) of Virtual Assets Act, 2025 of the Republic of Botswana for comprehensive use by the NBFIs. The note is indicative and while due care was exercised to ensure that this guideline is accurate and consistent with the FI Act, the latter shall prevail in the unfortunate case of ambiguity and NBFIRA does not guarantee or take any liability whatsoever.

Contents

PART I: INTRODUCTION

Authority

1. This *Guidance Note* is issued by the Non-Bank Financial Institution Regulatory Authority (NBFIRA), pursuant to Section 49 (1) (c) of the Financial Intelligence Act, 2022 as amended in 2025 (FI Act), read with Section 5 (2) (e) of the Non-Bank Financial Institution Regulatory Authority Act, 2023 (NBFIRA Act), which empowers the Authority to issue instructions or guidelines to help non-bank financial institutions (NBFIs/regulated entities) comply with the FI Act.

Purpose

2. The FI Act sets obligations for regulated entities including those conducting virtual assets business to detect and prevent the occurrence of financial crimes including money laundering, terrorism and proliferation financing (ML/TF/PF) within or through their operations. By raising awareness of their obligations and providing practical guidance, this document seeks to assist entities conducting virtual assets (VA) businesses including virtual assets service providers (VASPs) to effectively detect, prevent and report suspected financial crimes, and ensure compliance with regulatory requirements. It describes how the FI Act applies to the unique operational activities in the VA business to help entities better understand how they should implement FI Act obligations effectively.

Objectives

3. The key objectives of this Guidance Note are as follows;

(a) **Raise Awareness** among VA businesses regarding their obligations under the FI and VA Acts. By understanding their regulatory obligations, it is envisaged that VA businesses can take proactive steps to implement effective compliance measures.
(b) **Provide Clarity** on the key components of anti-money laundering, combatting

terrorism and proliferation financing (AML/CFT and PF) programmes, including customer due diligence (travel rule), transaction monitoring, and reporting of suspicious activities. With regulatory requirements clarified, VA businesses can consistently and comprehensively implement AML/CFT measures.

(c) **Offer Practical Guidance** and best practices for implementing AML/CFT programmes tailored to the unique characteristics of virtual assets and cryptocurrencies[1]. With actionable recommendations provided, VASPs can enhance the effectiveness of their compliance efforts.

(d) **Promote Collaboration** and information-sharing among VA businesses, regulatory authorities, and law enforcement agencies in combating financial crime. By fostering collaboration, entities can contribute to a collective effort to safeguard the integrity of the financial system.

Scope

4. This *Guidance Note* applies to entities licensed and supervised by the NBFIRA to conduct a virtual asset business. It specifies considerations for AML/CFT programme of a regulated entity. The guidelines are not intended to be exhaustive nor to set limits on steps to be taken by regulated entities to detect, prevent and report financial crimes.

Accountability and Responsibility

5. Governing bodies [or most senior management in the absence of the former] of NBFIs are ultimately accountable and responsible for their entity's compliance with provisions of the FI Act and all other financial services laws. The responsibility may be delegated to management to ensure compliance during day-to-day business activities as conducted by an entity.

[1] The Authority recognises and references various global standards in this guidance note, amongst them recommendations and guidelines issued by the Financial Action Task Force (FATF), International Organization of Securities Commissions (IOSCO), World Bank, and International Monetary Fund (IMF).

PART 2: VIRTUAL ASSETS AND VIRTUAL ASSETS BUSINESS (Introduction)

6. Virtual assets business markets are still relatively small compared to traditional financial markets, however, their global penetration and spread has so far remained unprecedented in the broader financial markets. This rise in use of virtual assets and cryptocurrencies has brought about a paradigm shift in the financial landscape, offering innovative solutions for digital transactions and investments. However, with this innovation comes the challenge of mitigating the risks associated with financial crimes, including money laundering, terrorism financing and proliferation financing.

7. These new technologies, while having varying distinctions, i.e., as crypto or virtual or digital currencies, have two main commonalities i.e. (a) not being under a central authority regulatory control and (b) being a representation of value and in digital form that can be invested, traded or exchanged for other assets through virtual trading platforms.

8. Botswana has not been spared of these developments. Observations indicate that individuals have been using and transacting virtual assets through web-based digital platforms operated by VASPs, some foreign-based. More recently, there have been local service providers providing platforms for the exchange, sale and transfers of virtual assets.

9. Supervision of VA businesses in Botswana began with promulgation of the VA Act in 2022[2] and the designation of VA businesses as NBFIs, thereby automatically subjecting them to other financial services laws and regulations including the FI Act, as specified parties. The 2023 National Risk Assessment (NRA) has classified

[2] VA Act 2022 was repealed and replaced by VA Act 2025

the Virtual Asset Service Providers (VASPs) sector as high risk. The designation carries significant implications for both VASPs and the Authority.

Virtual Assets

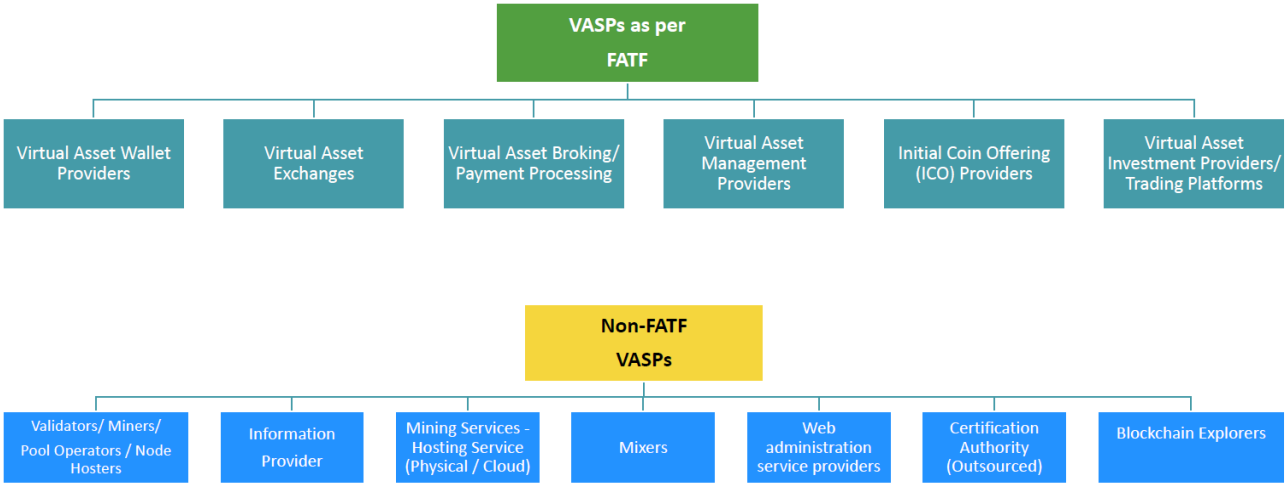
10. FATF defines virtual assets as digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. VA Act definition follows similar description and excludes digital representation of a central bank legal tender and securities or assets defined or regulated under Securities Act. The underlying distinction from other assets, say the Pula currency or securities, is that VAs, beyond just digital representation of value/asset, are tradeable and exchangeable for any asset only in digital form. Nonetheless AML/CFT controls, while recognising the peculiarity of VAs, should be applied on all VA businesses based on their basic characteristic that, similar to fiat currencies, they are an asset and or have an underlying value.

Virtual assets service providers

11. The VA Act adopts the FATF definition of VASPs which describes them as any person who; under an agreement, as part of a business, undertakes a virtual asset service or any of the following activities for or on behalf of another person — (a) the exchange between virtual assets and fiat currencies, (b) the exchange between one or more forms of virtual assets, (c) the transfer of virtual assets, (d) the safekeeping or administration of virtual assets or instruments enabling control over virtual assets, and (e) the participation in and provision of financial services related to an issuer's offer or sale of a virtual asset; or is a dealer or is willing to deal, on own account, by buying and selling virtual assets at prices set by that person, and includes a — (i) market maker or liquidity provider, (ii) system that provides virtual liquidity, allowing traders to buy and sell derivatives on the blockchain, or (iii) virtually automated market maker.

Types of VASPs

12. Under FATF standards, VASPs are broadly categorised into two; those that are subject to financial regulatory oversight including for compliance with AML/CFT requirements or those that are not any financial regulatory purview. The figure below shows VASPs that are recommended for oversight by the FATF and considered outside the financial sphere. Botswana's VA supervisory regime through the VA Act and other relevant legislation aligns its approach with that of the FATF.



PART 3: REGULATORY FRAMEWORK, STRATEGIES AND RELEVANT STANDARDS

Virtual Assets Act

13. The VA Act is the primary legislation for licensing of VASPs and regulation of virtual assets business activities for prudential and good market conduct. VA Act seeks to enhance transparency, accountability, and integrity in the virtual asset ecosystem, thereby fostering trust and confidence among stakeholders, including investors, consumers, and relevant supervisory authorities. Additionally, the Act seeks to promote innovation, market stability and growth within both the VA sector and the entire financial industry while guarding against the misuse of virtual assets for illicit

activities.

Financial Intelligence Act

14. The Financial Intelligence Act (FI Act)[3] is the apex legislation for prevention of financial crimes in Botswana. It provides obligations for entities to comply with the Act by detecting, preventing and reporting financial crimes. The Authority has summarised and sequenced these obligations into six (6) main duties; being (1) Governance (establishment of AML/CFT compliance oversight function including audit), (2) Risk Management System and Controls (risk assessment and policies), (3) Training (facilitating understanding of risks and controls), (4) Customer Due Diligence (includes enhanced due diligence), (5) Transaction Monitoring and Reporting (suspicious transaction process), and (6) Record Keeping (retention of CDD and transactional information). This Guidance Note is for the most part based on obligatory provisions of the FI Act.

Financial Action Task Force (FATF) Recommendations

15. The Financial Action Task Force (FATF) is an intergovernmental body established to set standards for the prevention and suppression of financial crimes. There are 40 Recommendations which must be adopted by both supervisory authorities and entities including VASPs. Recommendation 15 of FATF focuses on new technologies, particularly virtual assets and cryptocurrencies, and their potential use in money laundering, terrorism financing and proliferation financing. The recommendation emphasises the need for countries to ensure VASPs are subject to effective regulation and supervision, including measures to prevent their misuse for illicit purposes. This Guidance Note provides other applicable recommendations and FATF guidance papers such as Immediate Outcomes which relate to the 6 obligations under the FI Act.

[3] The FI Act has two Regulations: FI Regulations and FI (Implementation of United Nations Security Council Resolutions) Regulations.

National Risk Assessment Reports

16. Botswana's national risk assessment is conducted every five years. The exercise's output is a published comprehensive report intended for use by both public and private sectors to inform national and organizational strategies to prevent financial crimes. The country concluded its maiden national risk assessment in 2017, the report of which guided the country until 2023. At the time, however, the VA business sector in the country was considered to be in its nascent stage, therefore it was not assessed. The second NRA, which covered the 6-year period to 2022 and was concluded in 2023 and included VAs activities in scope . The NRA report indicated the sector's high-risk rating which indicated serious vulnerabilities [of the sector] and threats in the country, regionally and other parts of the world. The high-risk rating necessitates development of effective actions by both supervisors, law enforcement agencies, VASPs and entities dealing with VAs. The issuance of this Guidance Note is part of supervisory efforts to raise awareness on relevant regulatory obligations and applicable standards for VASPs and VA dealers to employ adequate controls.

Other References

17. This *Guidance Note* has also leaned on the following related laws and papers for guidance:

    (a) Counter Terrorism (Amendment) Act, 2022.
    (b) Data Protection Act, 2025
    (c) FATF Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Assets Service Providers (October 2021).
    (d) FATF Guidance on Digital Identity.
    (e) Targeted Update on Implementation of the FATF Standards on Virtual

Assets and Virtual Asset Service Providers (June 2022).

(f) Financial Action Task Force Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins (June 2020).

(g) Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (report by International Organization of Securities Commissions).

(h) Other guidance notes issued by the NBFIRA from time to time.

PART 4: VASPs AML/CFT OBLIGATIONS

Risk Assessment

18. Entities conducting VA businesses should adopt a risk-based AML/CFT approach (RBA) and conduct an institutional ML/TF/PF risk assessment to identify, assess and understand the level and nature of risk of commission of ML/TF/PF crimes and take appropriate measures to manage and mitigate the identified risks. Section 13 of the FI Act requires that risk assessment be conducted on customers, business relationships, pre-existing products/services, practices, and delivery mechanisms, new technologies, new business procedures, product delivery channels, countries/geographic areas. These risk areas can be extended to suit unique characteristics of an entity – the goal being to ensure that all relevant aspects of the business are covered.

19. It is mandatory that entities develop a standardised risk assessment methodology to be used to guide periodic assessment as this would allow for accurate observation and evaluation of risks over a period of time. This should, however, not be taken to mean that methodologies are constant – they may be reviewed and updated as and when the need arises. Risk assessment methodology should provide risk factors associated with features of financial services and products offered. The table below provides ML/TF/PF risk factors to be considered for VA

business risk assessment. These are not exhaustive and may apply to varying degrees for different VA businesses, products or services. An entity will need to employ its skills and understanding of business so that it is able to adequately capture surrounding threats, vulnerabilities of each service and product, as well as its AML/CFT obligations.

Risk Factor	Description
Anonymity	VAs and cryptocurrencies offer a certain level of anonymity, making it difficult to trace the flow of funds and identify the individuals involved in transactions. This masking increases with speed and transactions across multiple platforms and different VAs.
Pseudonymity	While transactions are recorded on a public ledger, participants are often identified by pseudonyms rather than their verified identities, providing a degree of privacy that can be exploited for illicit activities.
Global Accessibility	VAs and their platforms can be accessed from anywhere in the world with an internet connection, making it easy to elude national regulatory frameworks. The easiness of global reach is often a catapulting factor for mass adoption and eventual growth and high market capitalisation.
Cross-Border Transactions	Global accessibility of the VAs and cryptocurrencies is the main driver for a surge in cross-border transactions, in most cases, with no or minimal regulatory oversight, allowing illicit funds to be moved across borders quickly and with relative ease.
Lack of Regulation	The regulatory landscape surrounding virtual assets and cryptocurrencies is still in its infancy stage with many jurisdictions lacking comprehensive AML/CFT regulations and understanding of the sector. VAs may be kept in unhosted or non-custodial accounts/wallets where a customer controls its private keys, rather than an exchange or trading platform. This gives users full control of their own VA, rather than requiring permission from a third party. It also means there is no regulatory oversight of transactions, thus increasing vulnerability for illicit transactions.
Decentralisation	The decentralized nature of many cryptocurrencies means there is no central authority overseeing transactions, making it difficult to implement AML/CTF measures effectively.

Multiple/Bundled Services	Some cryptocurrencies offer bundled services that allow users to obfuscate the origin of their funds, making it harder to trace illicit activities.
Complex Transactions	Cryptocurrency transactions can involve multiple wallets, addresses, and exchanges, making it challenging for law enforcement agencies to follow the money trail.
Emerging Technologies	As new technologies and cryptocurrencies emerge, criminals may exploit vulnerabilities in these systems to engage in illicit activities.

20. Timing and frequency of risk assessment exercises is important as it ensures the entity is kept abreast of new ML/TF/PF risk trends and typologies. In line with the FI Act obligation to keep an up-to-date risk assessment, entities should conduct preliminary risk assessments prior to launch of product/service, commencement of a virtual assets business or change and introduction of new virtual coins, trading platform etc. And where there are changes within the business operations, business and regulatory environment, an ongoing update to the risk assessment shall be carried out to maintain understanding of emerging risks.

21. Upon completion of evaluation of risks, a control framework [comprising of AML/CFT/customer acceptance policies, systems, internal programs and procedures] must be developed to effectively identify suspicious transactions, transaction monitoring processes, implement and maintain a training policy, and record keeping policies.

Corporate Governance

22. The quality of corporate governance is critical in the assessment of risk management and compliance (policy and regulatory) with respect to AML/CFT. The organisational and business culture of an entity will largely depend on the type of corporate governance in effect and will set the tone for the conduct and management of risk across its significant activities, that is, business lines and operating units. Good corporate governance sets clear expectations for ethical

behavior, accountability, and transparency, and providing adequate resources and support for AML/CFT compliance efforts. Additionally, it ensures that the organisation's AML/CFT programme is aligned with regulatory requirements and industry best practices, enabling the institution to effectively combat financial crime and maintain the trust and confidence of its stakeholders. While VASPs may have different operating models, it is important to maintain clear management roles and responsibilities for accountability and risk management.

23. VASPs are obligated through Section 14 (1) (a) as read with Directive to Establish an AML/CFT Compliance Function (Directive 1) to have an independent and well-resourced AML/CFT compliance function. The entity must designate an AMLCO at management level who must meet NBFIRA fit and proper rules for key controllers and requirements of FI Act, and most importantly be approved by NBFIRA. The AMLCO will oversee the implementation of internal programmes and procedures, including maintenance of records and reporting of suspicious transactions, and ensure that the compliance officer always has timely access to customer identification data, transaction records and other relevant information. Entities should ensure that the size and competency of the compliance function is commensurate to the size and complexity of a business.

Customer Due Diligence

24. The FI Act[4] defines customer due diligence (CDD) as the process where relevant information about the customer is collected and evaluated for any potential risk of commission of financial offence. CDD also involves continuous monitoring of business relationships, including the due diligence information obtained, to ensure it remains up to date and that the relationship is operating as expected for that customer. VASPs are obligated to conduct CDD measures and ensure that the

[4] See s.2 of the FI Act

extent of the measures reflect a risk-based approach. This approach to customer identification will be guided by the specified party's risk assessment.

25. The FI Act requires entities to establish and verify the identity of beneficial owners when establishing a business relationship or carrying out a transaction with a customer. Where a VASP cannot apply the appropriate level of CDD, the VASP should not enter into a business relationship or carry out any transaction with the prospective customer.

26. VASPs should obtain and verify the customer identification/verification information required under national law. The required customer identification information usually includes information on the customer's name and further identifiers such as physical address, date of birth, and a unique national identifier number (e.g., national identity number or passport number), and any other ascertainment documentation or information prescribed by Regulation 6 (1) of FI Regulations.

27. VASPs should maintain controls and procedures for the protection of personal data and provide safeguards, confidentiality, and use of CDD information.

28. NBFIs should have in place CDD procedure that they effectively implement and use to identify and verify on a risk sensitive basis the identity of a customer, including when establishing business relations with that customer; where they have suspicions of ML/TF, regardless of any exemption of thresholds; and where they have doubts about the veracity or adequacy of previously obtained identification data.

29. For prominent influential persons (PIPs), VASPs must take reasonable measures to determine whether a customer or beneficial owner is a PIP and assess the risk of the business relationship. Furthermore, for higher-risk business relationships with domestic PIPs and international organization PIPs, VASPs should take

enhanced due diligence measures consistent with those applicable to foreign PIPs, including identifying the source of wealth and source of funds when relevant.

Travel Rule

30. Travel Rule relates to CDD requirements and mandates entities to collect and maintain CDD information of both the transaction initiating customer and receiving customer to enhance transparency. The VA Act[5] has legislated the FATF travel rule standard therefore mandating VASPs to ensure that they exchange customers' CDD information as transactions are conducted.

31. VASPs must obtain and hold originator and beneficiary information for transactions in the following detail.

(a) Originator Information: Collect and maintain accurate details about the sender of the virtual asset transfer. This includes:

(i) The name of the originator.

(ii) The originator's virtual asset wallet address or account number, or in the absence of an account, a unique transaction reference number.

(iii) The originator's physical address, national identity number, customer identification number, or date and place of birth.

(b) Beneficiary Information: Collect and maintain accurate details about the receiver of the virtual asset transfer. This includes;

(i) The name of the beneficiary.

(ii) The beneficiary's virtual asset wallet address or account number, or in the absence of an account, a unique transaction reference number.

(c) Submit Information Securely: Transmit the collected originator and beneficiary

[5] See s.26 of the VA Act

information immediately and securely to the beneficiary VASP or any other relevant institution as required by law.

(d) Storage of Information: Store the collected information in a manner that cannot be altered and ensure that the information is readily available to the Regulatory Authority upon request.

32. Required information for transfers involving natural persons;

(a) Transfers equal to or more than BWP 10,000:
    (i) Originator's name
    (ii) Originator's virtual asset wallet address or account number, or unique transaction reference number if no account exists
    (iii) Originator's physical address, national identity number, customer identification number, or date and place of birth
    (iv) Beneficiary's name
    (v) Beneficiary's virtual asset wallet address or account number, or unique transaction reference number if no account exists.

(b) Transfers less than BWP 10,000;
    (i) Originator's name
    (ii) Originator's virtual asset wallet address or account number, or unique transaction reference number if no account exists.
    (iii) Beneficiary's name
    (iv) Beneficiary's virtual asset wallet address or account number, or unique transaction reference number if no account exists.

33. Required information for transfers involving body corporates.

(a) Transfers equal to or more than BWP 10,000;
    (i) Originator's registered corporate name or trading name.

(ii) Originator's virtual asset wallet address or account number, or unique transaction reference number if no account exists

(iii) Either the originator's customer identification number or registered office address/primary place of business.

(iv) Beneficiary's name.

(v) Beneficiary's virtual asset wallet address or account number, or unique transaction reference number if no account exists.

(b) Transfers less than BWP 10,000;

(i) Originator's name

(ii) Originator's account number or unique transaction reference number if no account exists

(iii) Beneficiary's name

(iv) Beneficiary's account number or unique transaction reference number if no account exists.

34. Execution of Transactions

(a) Compliance Check: Ensure that each transaction complies with the required information criteria as set out above.

(b) Non-Compliance: Do not execute a transaction that does not meet these requirements. Instead, return the transaction amount to the originator.

(c) Risk-Based Policies: Implement appropriate risk-based policies and procedures to determine when to execute, reject, or suspend a transfer that lacks the required information. Always ensure compliance with these requirements.

35. Determining Transfer Value

(a) Use a reasonable and documented approach to determine the value of a transfer.

(b) For linked transfers, aggregate multiple transfers from the same originator that appear to be linked to calculate the transfer's total value.

36. Responsibilities of Intermediary VASPs

As an intermediary VASP participating in virtual asset transfers, you must:

(a) Identify Non-Compliant Transfers: Take reasonable measures, consistent with current guidance, to identify transfers that lack the required originator or beneficiary information.

(b) Risk-Based Policies: Adopt risk-based policies and procedures to determine when to execute, reject, or suspend a transfer that lacks the required information.

(c) Record-Keeping: Maintain records of transactions for at least 20 years after their completion.

37. Exemptions for Batch Transfers

When several transfers from a single originator are bundled in a batch file for transmission to beneficiaries, there may be an exemption from the requirements for individual originator information if the batch file includes the originator's account number or unique transaction reference number, and if it contains accurate originator information and full beneficiary information that is fully traceable within the beneficiary country.

38. Transfers to/from Self-Hosted Wallets

(a) Information Collection: Obtain and hold the required information as specified for natural persons and body corporates.

(b) Risk-Based Measures: If a transfer exceeds BWP 10,000 or if there is a suspicion of money laundering or terrorist financing, implement adequate risk-based measures to mitigate and manage these risks.

39. Compliance with the Travel Rule is essential to ensure transparency and security in virtual asset transactions. Adhering to these obligations helps detect and prevent illicit activities and fosters trust in the virtual asset ecosystem. Entities must

implement robust procedures, continuously monitor transactions, and stay informed about regulatory updates.

Transaction Monitoring

40. Financial criminals are increasingly adopting the use of VAs and VASPs to move their illicit funds between different jurisdictions with minimal detection. Such high level of ML/TF/PF risk should be considered by VASPs, and stringent controls should be in place for monitoring and reporting such forms of suspicious transactions.

41. Transaction monitoring entails scrutinising transactions to determine those that are consistent with an entity's information concerning the customer and the nature of the business relationship. The customer's behavior, use of products, and amounts involved are aspects of the customer profile that must be monitored. This makes it possible to identify transactions that are potentially suspicious or deviate from a customer's usual pattern of transactions. VASPs should have appropriate database systems and transaction monitoring systems that will be used for effective monitoring of transactions. The adequacy of monitoring systems and the factors that lead VASPs to adjust the level of monitoring should be reviewed regularly for continued relevance to their AML/CFT policy and risk assessment. As an example, high-risk and PIP customers should be placed under enhanced monitoring.

Reporting

42. VASPs should have adequate systems as mentioned above for transaction monitoring, and to have ability to flag for further analysis any unusual or suspicious movement of funds inclusive of those relating to VAs. Such transactions must be

scrutinised in a timely manner and determination can be made to whether funds are suspicious. The FI Act obliges VASPs to report (1) suspicious transactions reporting within 5 working days, (2) cash and (3) cross-border transactions equivalent and more than BWP 10 000. For efficient reporting, entities should create their profile and register on the goAML, a reporting platform administered by the Financial Intelligence Agency. The NBFIRA has previously issued a directive instructing entities to register on the goAML, and failure to do so may lead to a regulatory sanction.

Record Keeping

43. The FI Act requires that CDD information and transaction records be kept for 20 years after the establishment of a business relationship and transaction. Entities should maintain records obtained from their CDD measures, accounts files and business correspondence (i.e., transaction originator and recipient). Considering the span and specific details of this obligation, it is imperative that entities have in place appropriate and well backed up systems for record keeping.

Training

44. Effective implementation of internal controls is a product of good understanding of an organisation's risks and VASPs are obligated by the FI Act to conduct training for their staff on AML/CFT matters, current legislation, trends, emerging risks and mitigation controls, and other financial crime related matters concerning VA business.[6] An AMLCO should be formally trained on AML/CFT related certification, and must continuously familiarise themselves with business activities, AML/CFT obligations, FATF Recommendations and be accountable to training staff members.

[6] Directive 1 prescribes training subjects.

PART 5: CONCLUSION

Conclusion

45. It is expected that henceforth, all entities will follow the guidance note and apply appropriate levels of due diligence when engaging in VA business. VASPs are expected to have adequate risk management systems to ensure customers or entities that are appreciably exposed to money laundering risk, proliferation risk and terrorist financing risk are dealt with proportionately to prevent such risks from materialising. And for customers suspected of commission of financial crimes to be reported to the FIA for further guidance.

46. VASPs and other entities interested in engaging in VA business are advised to familiarise themselves with the prevailing FI Act, FATF Recommendations, Virtual Assets Act and its regulations, and other relevant laws in order to understand their legal obligations and ensure adequate compliance programs in line with Botswana legislation to combat money laundering, and the financing of terrorism and proliferation.

***