Financial Intelligence Centre
Republic of Namibia

PO Box 2882
Windhoek
Namibia

Phone: + 264 61 283 5286
Fax: + 264 61 283 5918
Helpdesk@fic.na

GUIDANCE NOTE NO. 10 OF 2023

GUIDANCE ON RISK ASSESSMENTS AND ML/TF/PF INDICATORS: VIRTUAL ASSETS SERVICE PROVIDERS AND INITIAL TOKEN OFFERINGS (ITO) PROVIDERS

First Issued: 30 June 2023

TABLE OF CONTENTS

A. DEFINITIONS AND ABBREVIATIONS

"Accountable Institution (AI)" means a person or entity listed in Schedule 1 of the Act;

"Administrator" is a person or entity engaged as a business in issuing (putting into circulation) a centralised virtual currency, establishing the rules for its use; maintaining a central payment ledger; and who has the authority to redeem (withdraw from circulation) the virtual currency;

"Anonymiser" (anonymising tool) refers to tools and services, such as darknets and mixers, designed to obscure the source of a Bitcoin transaction and facilitate anonymity. [Examples: Tor (darknet); Dark Wallet (darknet); Bitcoin Laundry (mixer)];

"Business relationship" means an arrangement between a client and an accountable or reporting institution for the purpose of concluding transactions on a regular basis;

"CDD" means Customer Due Diligence;

"Client and Customer" have their ordinary meaning and are used interchangeably herein;

"Cold Storage" refers to an offline Bitcoin wallet—i.e., a Bitcoin wallet that is not connected to the Internet. Cold storage is intended to help protect the stored virtual currency against hacking and theft. It is commonly referred to as an unhosted wallet;

"Customer Due Diligence" (CDD) means a process which involves establishing the identity of a client, the identity of the client's beneficial owners in respect of legal persons and monitoring all transactions of the client against the client's profile;

"Dark Wallet" is a browser-based extension wallet, currently available on Chrome (and potentially on Firefox), that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymiser (mixer); decentralised trading; uncensorable crowd funding platforms; stock platforms and information black markets; and decentralised market places similar to the so-called Silk Road;

"Enhanced Due Diligence" (EDD) means doing more than the conventional simplified due diligence or the basic CDD measures mentioned above and includes, amongst others, taking

measures as prescribed by the Centre to identify, as far as reasonably possible, the source of wealth, funds and any other assets of the client or beneficial owners whose activities may pose a risk of ML, TF or PF;

"Establish Identity" means a two-tier process consisting of *ascertainment or collecting* of certain identification information, and *verification* of some of the information against reliable documentation or information;

"FATF" means the Financial Action Task Force;

"FIA" refers to the Financial Intelligence Act, 2012 (Act No. 13 of 2012);

"FIC" means the Financial Intelligence Centre;

"Hot Storage" refers to an online bitcoin wallet. Because it is connected to the Internet, hot storage is more vulnerable to hacking/theft than cold storage. It is hosted by a service provider or entities that provide custodial services.

"LEAs" means Law Enforcement Authorities such as the Namibian Police, Anti-Corruption Commission or NAMRA;

"M**iner"** is an individual or entity that participates in a decentralised virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system. Miners may be users, if they self-generate a convertible virtual currency solely for their own purposes, e.g., to hold for investment or to use to pay an existing obligation or to purchase goods and services. Miners may also participate in a virtual currency system as exchangers, creating the virtual currency as a business in order to sell it for fiat currency or other virtual currency;

"Mixer" (laundry service, tumbler) is a type of anonymiser that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address;

"ML" means Money Laundering;

“PEPs” means Political Exposed Persons (See FIC Guidance Note 01 of 2019);

“PF” means proliferation financing;

“Records” means any material on which information is recorded or marked and which is capable of being read or understood by a person, or by an electronic system or other device;

“Regulations” refer to the FIA Regulations unless otherwise specified;

“RBA” refers to the Risk Based Approach. An approach for managing risks based on prioritization of such risks as per the occurrence/frequency/probability and potential impacts/consequences of each identified risk;

“SAR” refers to a suspicious activity report submitted to the FIC in terms of sections 33 (1) & (2) of the Act;

“Single Transaction” means a transaction other than a transaction concluded in the course of a business relationship;

“STR” refers to a suspicious transaction report submitted to the FIC in terms of sections 33 (1) & (2) of the FIA;

“TF” means Terrorist Financing;

“Tor” (originally, The Onion Router) is an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network’s users, by routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption. Tor makes it very difficult to physically locate computers hosting or accessing websites on the network;

“Transaction” means a transaction concluded between a client and an accountable or reporting institution in accordance with the type of business carried on by that institution, and includes attempted transactions;

"User is a person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal) investment. Users can obtain virtual currency in several ways. For example, they can (1) purchase virtual currency, using real money (from an exchanger or, for certain centralised virtual currencies, directly from the administrator/issuer); (2) engage in specific activities that earn virtual currency payments (e.g., respond to a promotion, complete an online survey, provide a real or virtual good or service); (3) with some decentralised virtual currencies (e.g., Bitcoin), self-generate units of the currency by "mining" them (see definition of miner, below), and receive them as gifts, rewards, or as part of a free initial distribution;

"Virtual Asset (VA)" VAs must be digital and must themselves be digitally traded or transferred and be capable of being used for payment or investment purposes. That is, they cannot be merely digital representations of fiat currencies, securities and other financial assets without an inherent ability themselves to be electronically traded or transferred and the possibility to be used for payment or investment purposes;

"VASPs" refers to Virtual Assets Service Providers. A VASP is a person who carries out one or more of the five categories of activity or operation described in the VASP definition below (i.e "exchange" of virtual/fiat, "exchange" of virtual/virtual, "transfer," "safekeeping and/or administration," and "participation in and provision of financial services related to an issuer's offer and/or sale");

"Virtual Asset Service Provider (VASP)" The definition of a VASP is broadly defined by the Financial Action Task Force (FATF), owing to the nature of virtual asset operations. Along such guidance, Namibia has adopted[1] a functional approach and applies the following concepts underlying the definition to determine whether an entity is undertaking the functions of a VASP. A VASP is any natural or legal person who, as a business, conducts one or more of the following activities or operations for, or on behalf of another natural or legal person:

i. Exchange between virtual assets and fiat currencies;
ii. Exchange between one or more forms of virtual assets;
iii. Transfer of virtual assets;

[1] the proposed FIA amendments and both FIC Directives 01 and 02 of 2021.

iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

"Without delay" means taking required actions within a few hours, as advised in Namibia's September 2022 Mutual Evaluation Report.

B. TYPICAL VASPs AND THEIR SERVICES

Virtual Asset Wallet Providers	Custodial	Hot Wallet
	Non-custodial	Cold Wallet
Virtual Asset Exchanges	Transfer Services	P2P
		P2B
	Conversion Services	Fiat-to-Virtual
		Virtual-to-Fiat
		Virtual-to-Virtual
Virtual Asset Broking/Payment Processing	Payment Gateway	ATMs
		Merchants
		Cards
Virtual Asset Management Providers	Funds	Fund Management
		Fund Distribution
		Compliance, Audit, and Risk Management
Initial Token/Coin Offering Providers	Fund raising	Fiat-to-Virtual
		Virtual-to-Virtual
	Investment	Development of Product and Services
	Other offerings	Security Token Offerings (STOs)
		Initial Exchange Offerings (IEOs)
Virtual Asset Investment Providers	Trading Platforms	Investment into VA-related commercial activities
		Non-Security Tokens and Hybrid Trading Activities
		Stablecoins
	Emerging Products	Crypto Escrow Service
		Crypto-Custodian Services
Validators/Miners/Administrators	Proof of Work	Fees New Assets

1. BACKGROUND

Virtual Assets (VA) and related services have the potential to spur financial innovation and efficiency but their distinct features also create new opportunities for Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF) activities. The ability to transact across borders rapidly not only allows criminals to acquire, move, and store assets digitally often outside the regulated financial system, but also to obfuscate the origin or destination of the funds, making it harder to identify suspicious activities in a timely manner. In comparison to the conventional fiat currency financial system, the VA space has increased anonymity and pseudonymity. These factors add hurdles to the detection and investigation of criminal activity by national authorities.

This guidance note will add to the framework of tools aimed at enhancing Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation (AML/CFT/CPF) measures at institutional, sectoral and national level. It is common cause that services offered by VASPs have been abused for ML domestically, as reflected through cases investigated. Internationally, there are trends and typologies which suggest such abuse to advance TF/PF activities.

This document avails sectoral guidance on conducting risk assessments and indicators of common ML, TF and PF activities. It contains Guidance on how Virtual Assets Service Providers (VASPs) should conduct ML/TF/PF risk assessments, as the starting point for implementing risk based mitigation systems. Risk assessment outcomes highlight risk levels and thus enable a VASP to prioritize its control implementation. Guidance Note 11 of 2023, issued along with this Guidance Note, provides essential guidance on how VASPs can effectively implement mitigating controls as per risks identified.

This Guidance Note is issued in terms of Section 9(1)(h) of the Financial Intelligence Act, 2012 (The FIA).as mentioned above, it is the first of two sectoral guidance notes for all persons who provide VA services within the definition of a VASP (see definitions sections herein above). At the time of issuing these guidance notes, the FIA amendments as well as VA and Initial Tokens Offerings Bill are on the verge of being passed in parliament.

2. SOURCES OF INFORMATION

This Guidance[2] relied on information from FIC's FIA Compliance Assessments, various national and sectoral risk assessments conducted over the years and the FATF's Updated Guidance for a Risk Based Approach for VASPS[3] on amongst others.

3. COMMENCEMENT

This Guidance Note comes into effect on **03 July 2023**.

4. SCOPE OF VASPs

4.1 Specific Services

Not all services offered within the VA space are vulnerable to abuse for ML, TF and PF risks. The AML/CFT/CPF framework as per the FIA and international standards only designates or limits the scope to services deemed vulnerable to risks of ML, TF and PF risks. Services of a support nature such as those of a miner on a conventional Bitcoin blockchain are not within the scope unless the miner starts availing any of the designated services.

The definitions section herein above defines VAs and VA operations which fall in the regulated definition. It lists the following five components or types of VA services that would make the provider of such services a VASP and thus an Accountable Institution as per the FIA: *Exchange between virtual assets and fiat currencies; Exchange between one or more forms of virtual assets; Transfer of virtual assets; Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.*

[2] Along with FIC Guidance 11 of 2023 which also relied on the same sources of information;
[3] Updated Guidance for a Risk Based Approach for VASPs: file:///C:/Users/ham638/Downloads/Updated-Guidance-VA-VASP%20(1).pdf and the FATF Report – Virtual Assets Red Flags Indicators: file:///C:/Users/ham638/Downloads/Virtual-Assets-Red-Flag-Indicators%20(1).pdf

At the time of issuing this Guidance, the two VASPs registered with the FIC and active within the industry only avail services of buying and selling VAs. No other exchange, custodial, nor Initial Token Offering (ITO) services are provided domestically. This could change given the entities placed in the regulatory sandbox of the Bank of Namibia and enquiries received directed to the FIC.

4.2 Transactions Above the Threshold

The FIA is informed by international instruments which lay the foundation for how Namibia and all other countries should contribute to international ML/TF/PF risk management in safeguarding our financial system. The FATF Recommendations inform the provisions of the FIA.

Only transactions above the prescribed threshold of NAD 5,000.00 should be subjected to CDD to combat ML. Note however that all transactions for designated services should be subjected to Targeted Financial Sanctions as per Directive 01 of 2023 (commencing with sanctions screening). At the time of this publication, the said threshold is being revised and indications are that it will be increased. Publications will be issued after finalisation of same.

VASPs need to keep in mind the need to identify related multiple cash transactions in excess of such threshold as those attempting to circumvent such controls can structure transactions below such CDD thresholds. At the time of issuing this document, national efforts are at an advanced stage to revise and possibly increase such threshold.

5. STAGES OF ML IN VASPs

There are different methods employed to advance ML but the main stages thereof remain the same. The following are generally the main stages of ML:

A. Placement

Involves placing the proceeds of crime in the financial system. *For example, buying or exchanging VAs with proceeds of crime shows placement of illicit proceeds.*

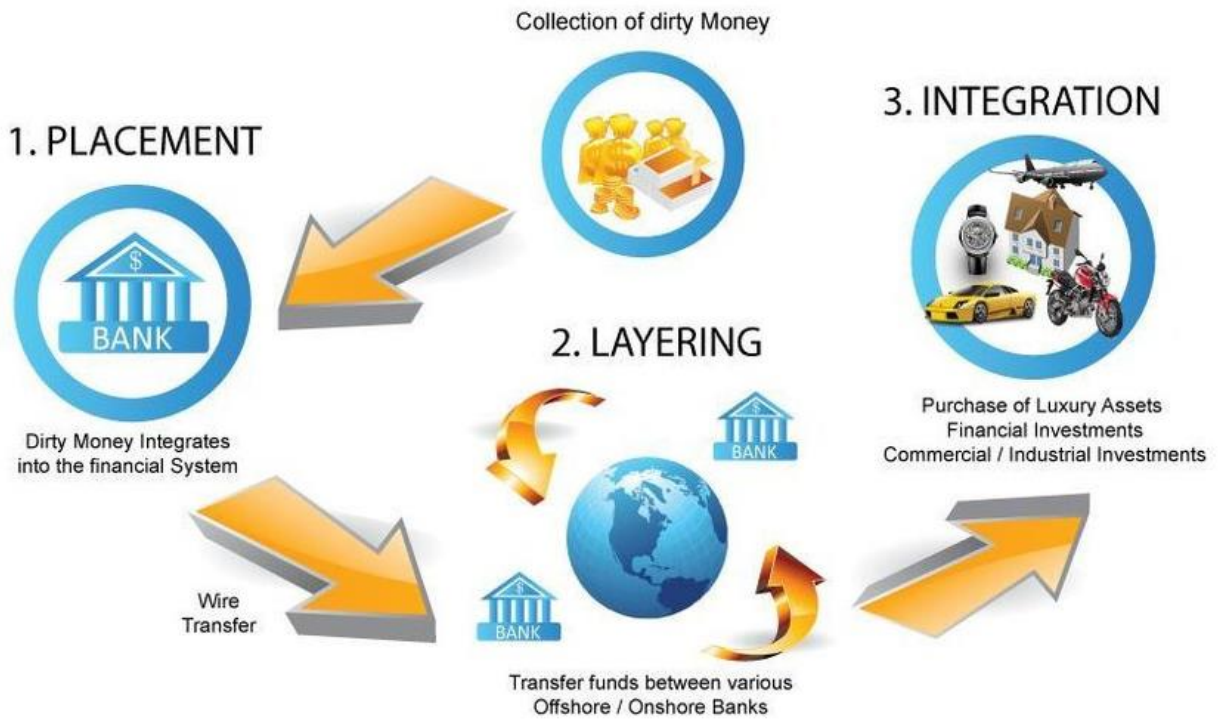
B. Layering

Involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds. The aim is usually to create as much distance as possible between the illicit activity/criminal and the illegal proceeds. *As the next step to the example indicated in A above, such proceeds from the sale are used to buy properties, invest in other VAs- in legitimate entities etc. These activities further distance such proceeds from its initial illicit activities.*

C. Integration

Usually the last stage of the ML process. Integration is at times similar to, or part of the layering process. The aim is to place the laundered proceeds back in the financial system under a veil of legitimacy.

Below is a diagram of the three main stages of ML.



VASPs, as part of their risk assessment process, should assess the ML/TF/PF vulnerabilities and high-risk factors associated with each of their products/services and delivery channels including counterparties (herein includes third parties playing similar role). The risk assessment guidance herein below also highlights indicators of potential high risks. Such should be considered, along with other variables, when conducting risk assessments at institutional level.

6. TF RISKS IN VASP

While the 2012 National Risk Assessment (NRA), 2017/18 update and 2020 NRA rightly observed that ML risks are more frequent and prominent, TF and similarly PF risks cannot be overlooked. It is well established that ML control vulnerabilities can be equally exploited to advance TF or PF activities. For this reason, controls that may be traditionally viewed as necessary for ML are equally essential for preventing and combatting TF and PF activities. This section speaks to TF risk considerations which are also similar for PF.

6.1 Nature of TF

As mentioned herein above, the characteristics of TF can make it difficult to identify. Worse, the VA space is clouded with enhanced anonymity and pseudonymity. The methods used to monitor ML can also be used for TF, as the movement of TF funds often relies on similar methods (control vulnerabilities) used for ML. Internationally, TF processes are considered to typically involve the following three stages:

a. *Raising funds* (through donations, legitimate wages, selling items, criminal activity);
b. *Transferring funds* (to a terrorist network, to a neighbouring country for later pick up, to an organisational hub or cell); and
c. *Using funds* (to purchase weapons or bomb-making equipment, for logistics, for compensation to families, for covering living expenses)

The risks associated with TF are highly dynamic. As such, VASPs need to ensure that their prevention and combatting measures are current, regularly reviewed and flexible. It is important to maintain preventative and combatting awareness as well as effective transaction monitoring systems that incorporate dynamic TF risks, along the more static risks associated with ML. The above considerations are similar for PF.

6.2 Transnational[4] Risks of TF

The 2020 NRA and 2023 NRA update observe that whilst Namibia is not considered high-risk for TF, even small-scale financing raised from within Namibia could have a significant impact if combatting measures fail. When looking at the risk of non-Namibian clients, VASPs should consider not only high-risk countries but also their neighbouring countries, as TF often involves the movement of funds or assets across borders. The 2020 NRA in particular, equally found that Namibia's porous borders present a significant vulnerability

[4] Extending or operating across national boundaries

which enhances the ease with which proceeds can be moved in and out of the country. VAs are borderless and thus highly vulnerable to TF abuse. Generally, control vulnerabilities exploited by TF threats can be similarly exploited by PF threats. This context is helpful to bear in mind in this section as VASP equally have an obligation to combat PF.

6.3 Namibia as a Conduit for TF

Despite the absence of domestic terrorism, the enhanced TF risks associated with foreign clients, especially those from high-risk countries, who are involved in precious metals and stones cannot be overemphasized. One of the potential consequences of transnational ML is that channels may be established that may also be exploited by terrorist and proliferation financiers. Overseas groups may seek to exploit Namibia as a source or conduit for funds to capitalise on Namibia's reputation as being a lower risk jurisdiction for TF. For instance, funds originating in or passing through Namibia may be less likely to attract suspicion internationally.

The same methods explained above through which VASPs can be abused to advance TF are similar for PF. The due diligence and RBA, especially screening of clients/parties to transactions against sanctions lists is essential in combatting both TF and PF within the sector.

6.4 Nature/Sources of TF funds

Funds that are used in TF (and PF) may be derived from either criminal activity or may be from legitimate sources, and the nature of the funding sources may vary according to the type of terrorist or proliferation organisation. Where funds are derived from criminal activity, the traditional monitoring mechanisms that are used to identify ML (as explained in this Guidance and Guidance Note 11 of 2023) may be appropriate for detecting potential TF, though the activity, which may be indicative of suspicion, may not be readily identified as or connected to TF.

6.5 Value/Size of Funds in TF

Transactions associated with TF may be conducted in very small amounts, which in applying a risk-based approach could be the very transactions that are frequently considered to be of minimal impact/risk with regard to ML. This is a bigger challenge for VAs and VASPs that do not naturally deal in financial services. Where funds are from legal sources, it is even more difficult to determine if they could be used for terrorist purposes. The need to be mindful of ML indicators for TF is valuable but a VASPs' AM/CFT policy/procedures have to deliberately distinguish controls aimed at detecting potential TF.

6.6 Covert Nature of TF Suspicions

The actions of those supporting terrorist and proliferation activities may be overt (openly) and outwardly innocent in appearance, such as the purchase of shell, or shelf[5] companies or take-over of existing businesses to further their goals, with the only covert (hidden) fact being the intended criminal use of such legal persons. Therefore, while terrorist funds may be derived from criminal activity as well as from legitimately sourced funds, transactions related to TF may not exhibit the same traits as conventional ML, and thus not easy to detect.

TF covers a wide range of terrorism-related activity, including operational funds, equipment, salaries and family compensation, social services, propaganda (e.g radicalization), training, travel, recruitment and corruption. However, in all cases, it is not the responsibility of the VASP to *determine the type of underlying criminal activity or intended terrorist, nor proliferation purpose* as a pre-requisite for reporting TF or PF suspicions. The VASP's role is to simply identify, report the suspicion without delay, freeze any VAs, funds or assets of such subject, while treating same with the necessary sensitivity. The FIC and relevant Law Enforcement Authorities have the responsibility to

[5] "Shell company" means an incorporated company with no independent operations, significant assets, ongoing business activities or employees. "Shelf company" means an incorporated company with inactive shareholders, directors, and secretary, which has been left dormant for a longer period even if a customer relationship has already been established.

investigate the matter further and determine if there is actual link to terrorism or proliferation activities. The misguided view to first want to establish an actual link to terrorism before filing any report has often exposed us to risks and not helped combating authorities to respond timely and promptly.

6.7 TF Risks Associated With NPOs

It is internationally accepted that some NPO-types or their services can be easily abused to advance terrorism activities. This typically happens with NPOs abusing the legitimacy and social trust that the sector enjoys for resourcing or financing terrorist activities directly or indirectly. In Namibia[6], charities and Faith Based Organizations (FBOs) were identified as the high-risk sub-sector within NPOs. VASPs need to apply the necessary level of due diligence when availing their services or dealing in one way or the other with NPOs, especially the types of NPOs specified herein to be higher risk for TF.

Amongst other controls, VASPs have to ensure due identification of ultimate beneficial owners of such NPOs and obtain information to gain assurance that proceeds or values related to such NPO/deals are not linked with persons associated with terrorism activities. It is also helpful to gain assurance that such NPOs are not subject to adverse reports around their governance frameworks, nor have associations with high-risk countries or terrorist groups.

6.8 Potential Origins of TF Threats

As per the various domestic SRAs, NRAs and consideration of TF trends internationally, the FIC highlights the following as primary TF threats VASPs should consider:

a. *Overseas groups able to inspire support through ideology* – Individuals may be inspired to contribute to overseas-based terrorist groups by travelling to conflict zones, which requires self or counterparty funding. Radicalised individuals may

[6] 2020 NRA.

also choose to contribute to terrorism by raising and contributing funds. VAs can be a source for raising funds or themselves easily transmitted or smuggled to where they are needed. This is the overarching context to keep in mind for TF purposes;

b. *Well-resourced groups with established networks* – This may involve the movement of larger sums of money for terrorism, in particular for or by state-sponsored groups; and
c. *Domestic terrorism* – given the low-to-non-existent level of domestic support for terrorist causes and absence of known terrorist networks, it is more likely that financiers of domestic terrorism (if it were to happen domestically) could manifest in Namibia as isolated disaffected individuals or small groups.

VASPs need to duly identify their clients, assess their risk profiles to minimize abuse from those who may be radicalized or somehow use legal persons and arrangements to move or raise funds to advance TF.

6.9 Helpfulness of ML controls for TF

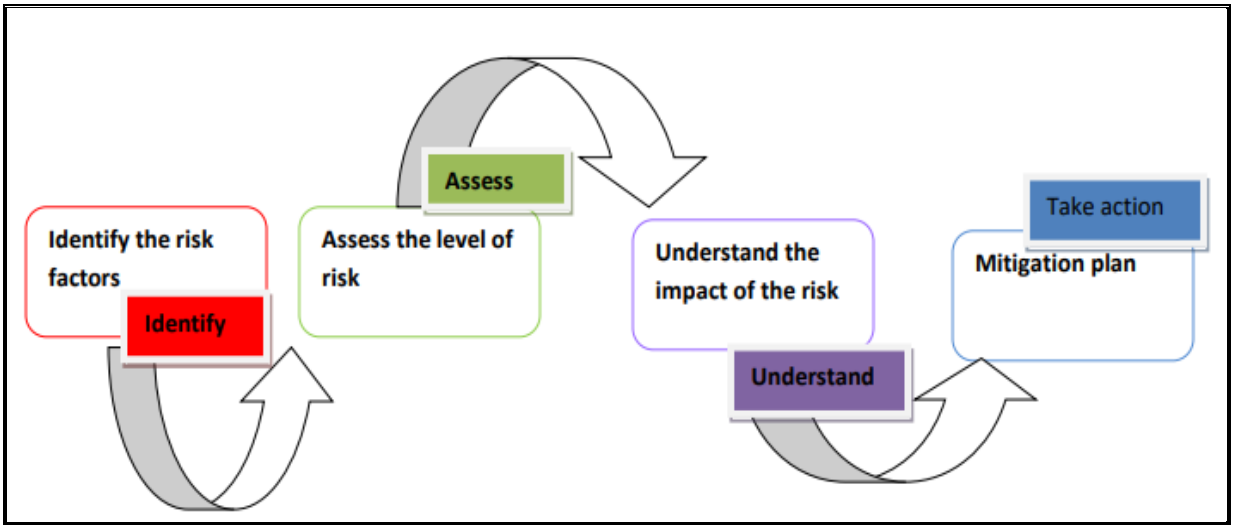
There are both similarities and differences in the application of the RBA to TF and PF on the one hand and ML on the other. They both require a process for identifying and assessing risk. However, the characteristics of TF make its detection and the implementation of mitigation strategies challenging due to considerations such as the relatively low value of transactions involved in TF, or the fact that funds can be derived from legitimate as well as illicit sources. Namibia has not observed potential TF exposure within the VASP sector. This does not however mean the sector is not vulnerable to such abuse[7]. The international trade of precious metals and stones, given their exposure to foreign clients, some of whom may have ties to high terrorism risk jurisdictions or have ties to terrorist organizations, remains inherently[8] vulnerable to TF abuse.

[7] ESAAMLG study also confirms that although the study has not conclusively confirmed a linkage between TF and proceeds of illicit dealing in PMS in the ESAAMLG region and in particular rubies in Northern Mozambique, the possibility cannot completely be ruled out as there are other studies by various researchers who have drawn linkages between rubies and TF. No information was provided by Mozambique that could have helped in establishing a link or none thereof between the illicit dealing in PMS and TF activities.
[8] Inherent risks refer to the level of (original) risks prior to the implementation of controls to reduce the likelihood and impact of such risks.

7. UNDERSTANDING THE RISK BASED APPROACH (RBA)

The basic intent behind the VASPs FIA obligations as derived from international standards is to ensure that VASP services and operations are not abused for facilitating criminal activities and ML/TF/PF.

The RBA speaks to a control system premised on a VASP's understanding of risks it may be exposed to. As shown in the diagram below, such understanding is what informs the design, nature and extent of controls implemented to mitigate risks (mitigation plan). The key RBA features are: identifying risks, assessing such risks to understand their levels and impact, followed by a mitigation plan aligned to such risk levels. An effective control implementation is also characterised by documenting ML/TF/PF risk findings (in a risk report) and updating such when the need arises. This enables a platform through which risks are tracked.



Risk Based Approach implementation framework

The primary RBA steps can be explained as follows:

a. *identifying ML/TF risks facing a VASP:* this should be done with consideration of its customers, services, countries of operation, delivery channels and third parties. Such should be considered with regard to publicly available information related to

ML/TF risks and typologies. This process also ensure risks are duly *assessed*, classified or rated to enhance *understanding* of such. The understanding of risks lays the foundation for implementing risk management measures;

b. *Risk management and mitigation:* identifying and applying measures to effectively and efficiently mitigate and manage ML/TF/PF risks. Guidance Note 11 of 2023, issued along with this guidance explains how to implement risk based controls on the understanding of relevant risks;
c. *Ongoing monitoring:* implementing policies, procedures and information systems to monitor changes to ML/TF/PF risks; and
d. *Documentation:* documenting risk assessments, strategies, policies and procedures to monitor, manage and mitigate ML/TF risks.

The above suggests that access to accurate, timely and objective information on ML/TF/PF risks is a prerequisite for an effective RBA. If duly implemented, the RBA ensures prudent balancing of compliance costs to business and customers by prioritising and directing controls to where they are most needed, in a prudent manner. This ensures high risk clients and services are accorded controls which are commensurate to such risk levels while lower risk clients and services are not burdened with unwarranted stringent customer due diligence.

8. FOUNDATION OF THE RBA: CONDUCTING RISK ASSESSMENTS

The object of understanding client and transaction risks is to help the VASP determine the level of due diligence such client, transaction and if need be, third parties, should be subjected to. The principle in AML/CFT/CPF due diligence is that low risk clients making use of low risk services should be subjected to minimum or simplified due diligence. On the other hand, higher risk clients should be subjected to Enhanced Due Diligence (EDD). The nature and extent of EDD is dependent on the level of assurance/comfort that a VASP needs to gain in reducing its ML/TF/PF risk exposure.

VASPs, like all other sectors are best placed to understand their risk exposure and thus implement controls to manage same. This section avails basic guidance around carrying out a risk assessment as a foundation for the RBA.

8.1 Undertaking ML/TF/PF Risk Assessments[9]

The 2020 NRA rated the sector's ML vulnerability amongst the highest across all sectors. The lack of adequate AML/CFT controls at the time largely contributed to this. At individual entity level, the comprehensiveness of risk assessments should be aligned to the nature, complexity and risk exposure of a VASPs operations, in view of its products/services and third parties (or amendments to such). ML/TF/PF risks can be organised into the following primary categories: client risk profiles; risks associated with products/services and delivery channels; as well as country/geographic risks. The risks and red flags listed in each category herein below are not exhaustive but provide a starting point for VASPs to use when assessing risks or designing their RBA.

One indicator or red flag may not necessarily, on its own, suggest an illicit transaction. For example, the use of a hardware or paper wallet may be legitimate as a way to secure VAs against thefts but could be viewed by some as increasing ML risks. The presence of high risk indicators or red flags should be considered in the context of other characteristics about the customer and relationship, or a logical business explanation.

8.1.1 Red flags related to anonymity

In the examples given below, the client (or user), within the context of this Guidance also includes the third party or counterparty of the VASP. The most essential risk management

[9] FIA section 39(1) [Read with FIA section 23]: An accountable institution, on a regular basis, must conduct ML/TF/PF activities risk assessments taking into account the scope and nature of its clients, products and services, as well as the geographical area from where its clients and business dealings originate. Persons much measure, rank or rate (e.g low, medium and high) their level of risk for relevant elements of the services they aim to provide. You should rank each service as low, medium or high risk. The control measures should describe how the entity will reduce each level of risk, especially the medium and higher risk rated levels. The FIC may, in its interpretation however disagree with ratings not duly informed and request reconsiderations accordingly.

approach with VAs is to screen or review the trail of hobs/blocks on the blockchain to see the engagements a wallet may be linked to.

This set of indicators below draws from the inherent characteristics and vulnerabilities associated with the underlying technology of VAs. The various technological features below increase anonymity and add hurdles to the detection of criminal activity by LEAs. These factors make VAs attractive to criminals looking to disguise or store their funds. The following are worth noting:

a. *Transactions by a customer involving more than one type of VA, despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced cryptocurrency (AEC) or privacy coins;*
b. *Moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin;*
c. *Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of VA transfers on its customer's behalf, and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions. P2Ps are only easier identified when the VASP reviews the blockchain history of a wallet/client;*
d. *Abnormal transactional activity (level and volume) of VAs cashed out at exchanges from P2P platform-associated wallets with no logical business explanation;*
e. *VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms;*
f. *The use of Tor (originally, The Onion Router). Tor is an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network's users, by routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption. Tor makes it very difficult to physically locate computers hosting or accessing websites on the network. This difficulty can be exacerbated by use of additional tumblers or anonymisers on the Tor network. Tor is one of several underground distributed computer networks,*

often referred to as darknets, cypherspace, the Deep web, or anonymous networks, which individuals use to access content in a manner designed to obscure their identity and associated Internet activity;

g. *The use of Dark Wallets. A dak wallet is a browser-based extension wallet, currently available on Chrome (and potentially on Firefox), that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymiser (mixer); decentralised trading; uncensorable crowd funding platforms; stock platforms and information black markets; and decentralised marketplaces similar to Silk Road;*

h. *Mixers and tumblers: A mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then "comingles" this transaction with other user transactions, such that it becomes unclear to whom the user intended the funds to be directed. (Examples: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundry; Bitlaunder; Easycoin).*

Case Study: Use of mixing and tumbling – Helix

A darknet-based VASP, Helix, provided a mixing or tumbling service that helped customers conceal the source or owners of VAs for a fee over a three-year period. Helix allegedly transferred over 350,000 Bitcoin, with a value at the time of transmission of over USD 300 million.

The operator specifically advertised the service as a way to conceal transactions on the darknet from law enforcement. In February 2020, criminal charges including ML conspiracy and operating an unlicensed money transmitting business were brought against an individual who operated Helix. Helix partnered with the darknet marketplace AlphaBay until AlphaBay's seizure by law enforcement in 2017.

i. *Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports;*
j. *The use of decentralised/unhosted, hardware or paper wallets to transport VAs across borders;*
k. *Users entering the VASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domain names;*
l. *Users entering the VASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs. Transactions between partners using various anonymous encrypted communication means (e.g. forums, chats, mobile applications, online games, etc.) instead of a VASP;*
m. *A large number of seemingly unrelated VA wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other;*
n. *Use of VAs whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes;*
o. *Receiving funds from or sending funds to VASPs whose CDD or know-yourcustomer (KYC) processes are demonstrably weak or non-existent;*
p. *Using VA ATMs/kiosks –*
    i. *despite the higher transaction fees and including those commonly used by mules or scam victims; or*
    ii. *in high-risk locations where increased criminal activities occur. A single use of an ATM/kiosk is not enough in and of itself to constitute a red flag, but would if it was coupled with the machine being in a high-risk area, or was used for repeated small transactions (or other additional factors).*

Case Study: Use of IP address associated with Darknet Marketplace (AlphaBay example)

AlphaBay, the largest criminal darknet market dismantled by authorities in 2017, was used by hundreds of thousands of people to buy and sell illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals over a two-year span.

The site operated as a hidden service on the TOR network to conceal the locations of its underlying servers as well as the identities of its administrators, moderators, and users. AlphaBay vendors used a number of different types of VAs, and had approximately 200 000 users, 40 000 vendors, 250 000 listings and facilitated more than USD 1 billion in VA transactions between 2015 and 2017.

In July 2017, the U.S. Government, with assistance from foreign counterparts, took down the servers hosting the AlphaBay marketplace, arrested the administrator, and pursuant to a seizure warrant issued in the Eastern District of California, seized the physical and virtual assets from the marketplace itself, and those that represented the unlawful proceeds from the AlphaBay criminal enterprise. Federal agents obtained the warrants after tracing VAs transactions originating from AlphaBay to other VA accounts and identifying bank accounts and other tangible assets controlled by the alleged administrator

8.1.2 Red Flag Indicators about Senders or Recipients

This set of indicators is relevant to the profile and unusual behaviour of either the sender or the recipient of the illicit transactions.

8.1.2.1 Irregularities that may be observed during account creation

a. *Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs;*
b. *Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious;*
c. *Trying to open an account frequently within the same VASP from the same IP address; and*
d. *Regarding merchants/corporate users, their Internet domain registrations are in a different jurisdiction than their jurisdiction of establishment or in a jurisdiction with a weak process for domain registration.*

8.1.2.2 Irregularities that may be observed during CDD process

a. *Incomplete or insufficient KYC information, or a customer declines requests for KYC documents or inquiries regarding source of funds;*
b. *Sender / recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty;*
c. *Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process.*

8.1.2.3 Profile

a. *Politically Exposed Persons (PEPs): This includes both domestic and international (PEPs). All PEPs are inherently high risk for ML/TF. PF risk is not excluded. Foreign PEPs naturally present a higher risk than domestic PEPs as their CDD information cannot be effectively or readily verified with relevant domestic authorities. PEPs need to be subjected to EDD which include obtaining management approval before facilitating deals involving them, as per FIC Guidance Note 01 of 2019 and Guidance Note 11 of 2023;*
b. *A customer provides identification or account credentials (e.g. a non-standard IP address, or flash cookies) shared by another account;*
c. *Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated;*

d. *A customer's VA address appears on public forums associated with illegal activity; and*
e. *A customer is known via publicly available information to law enforcement due to previous criminal association.*

Case Study: Customer profile does not match with regular high-value VA trading

A VASP (exchanger) and an Financial Institution (payment institute) filed STRs with the FIU concerning a high value of VA trading that began when the account at the exchanger was opened. Specifically, the account holder had been carrying out various VA buying and selling transactions for over EUR 180 000 – which did not match the profile of the account holder (including occupation and salary).

Analysis found that the VAs were subsequently used for (i) transactions on a darknet market; (ii) online betting; (iii) transactions with VASPs that did not have adequate AML/CFT controls or that were under previous ML investigations involving millions of dollars; (iv) operations on platforms that offered peer-to-peer transactions of VAs; and (v) "mixing". The account holder had also made use of a variety of different means (e.g. money transfer, online banking, and prepaid cards) to move a consistent amount of funds out of his account in the same time frame.

The funds received by the account holder appeared to come from a network of individuals who bought VAs (Bitcoin) in cash and were located in different jurisdictions in Asia and Europe (including Italy), both via money transfer and the banking system. He also received funds on his prepaid cards from subjects in Africa and the Middle East, who in turn collected funds from fellow citizens residing in Italy and abroad. These funds were then used for cross-border transfers and online gambling, and were withdrawn in cash from ATMs in Italy.

8.1.2.4 Profile of potential money mule or scam victims

a. *Sender does not appear to be familiar with VA technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers, or scam victims turned mules who are deceived into transferring illicit proceeds without knowledge of their origins;*
b. *A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a VA money mule or a victim of elder financial exploitation;*
c. *A customer being a financially vulnerable person, who is often used by drug dealers to assist them in their trafficking business;*
d. *Customer purchases large amounts of VA not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a scam victim.*

8.1.2.5 Other unusual behaviour

a. *A customer frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a customer;*
b. *A customer tries to enter into one or more VASPs from different IP addresses frequently over the course of a day;*
c. *Use of language in VA message fields indicative of the transactions being conducted in support of illicit activity or in the purchase of illicit goods, such as drugs or stolen credit card information; and*
d. *A customer repeatedly conducts transactions with a subset of individuals at significant profit or loss. This could indicate potential account takeover and attempted extraction of victim balances via trade, or ML scheme to obfuscate funds flow with a VASP infrastructure.*

8.1.3 Red Flag Indicators in the Source of Funds or Wealth

The misuse of VAs often relates to criminal activities, such as illicit trafficking in narcotics and psychotropic substances, fraud, theft and extortion (including cyber-enabled crimes). Below are common red flags related to the source of funds or wealth linked to such criminal activities:

a. *Transacting with VA addresses or bank cards that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites;*
b. *VA transactions originating from or destined to online gambling services;*
c. *The use of one or multiple credit and/or debit cards that are linked to a VA wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing VAs are sourced from cash deposits into credit cards;*
d. *Deposits into an account or a VA address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds;*
e. *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 Initial Token/Coin Offering (ITO/ICO) where personal data of investors may not be available or incoming transactions from online payments system through credit/pre-paid cards followed by instant withdrawal;*
f. *A customer's funds which are sourced directly from third-party mixing services or wallet tumblers;*
g. *Bulk of a customer's source of wealth is derived from investments in VAs, ICOs, or fraudulent ICOs, etc.; and*
h. *A customer's source of wealth is disproportionately drawn from VAs originating from other VASPs that lack AML/CFT controls.*

8.1.4 Red Flag Indicators Related to Geographical Risks

This set of indicators emphasises how criminals, when moving their illicit funds, have taken advantage of the varying stages of control implementation by jurisdictions. The FATF[10] opines that based on cases reported by jurisdictions, criminals have exploited the gaps in AML/CFT regimes on VAs and VASPs by moving their illicit funds to VASPs domiciled or operated in jurisdictions with non-existent or minimal AML/CFT regulations on VAs and VASPs. These jurisdictions may not have a registration/licensing regime, or have not extended STR requirements to cover VAs and VASPs, or may not have otherwise introduced the full spectrum of preventive measures as required by the FATF Standards. These risks are associated with source, destination, and transit jurisdictions of a transaction. They are also relevant to risks associated with the originator of a transaction and the beneficiary of funds that may be linked to a high-risk jurisdiction. In addition, they may be applicable to the customer's nationality, residence, or place of business.

a. *Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located;*
b. *Customer utilises a VA exchange or foreign-located MVTS in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for VA entities, including inadequate CDD or KYC measures;*
c. *Customer sends funds to VASPs operating in jurisdictions that have no VA regulation, or have not implemented AML/CFT controls; and*
d. *Customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing VAs, or sets up new offices in jurisdictions where there is no clear business rationale to do so.*

[10] (FATF Report on VASP Red Flag Indicators)

What makes a jurisdiction high risk?

Information about high-risk jurisdictions is widely available, which is detailed from several open-source documents and media. The following are indications, based on credible sources, which may escalate the risk of a country that clients to a transaction may be associated with. Amongst other considerations, these are jurisdictions:

a. *that have been found by organisations such as FATF, World Bank, Organisation for Economic Cooperation and Development (OECD) and the International Monetary Fund as* ***not having effective AML/CFT/CPF measures*** *in place;*

b. *identified to be* ***uncooperative in extraditions and providing beneficial ownership information*** *to competent authorities, a determination which may be established from reviewing FATF Mutual Evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards; and*

c. ***Identified higher risk countries:*** *this may include conflict zones, countries subject to sanctions, embargoes issued by the international community including the UN, OFAC, EU etc. Also includes FATF greylisting or blacklisting.*

8.1.5 Red Flag Indicators Related to Transactions

8.1.5.1 Size and frequency of transactions

a. *Structuring VA transactions (e.g. exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions;*
b. *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, which is particularly common in ransomware-related cases; or*
- ✓ *to a newly created or to a previously inactive account.*

c. *Transferring VAs immediately to multiple VASPs, especially to VASPs registered or operated in another jurisdiction where –*
   - ✓ *there is no relation to where the customer lives or conducts business; or*
   - ✓ *there is non-existent or weak AML/CFT regulation.*

d. *Depositing VAs at an exchange and then often immediately –*
   - ✓ *withdrawing the VAs without additional exchange activity to other VAs, which is an unnecessary step and incurs transaction fees;*
   - ✓ *converting the VAs to multiple types of VAs, again incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification); or*
   - ✓ *withdrawing the VAs from a VASP immediately to a private wallet. This effectively turns the exchange/VASP into an ML mixer.*

e. *Accepting funds suspected as stolen or fraudulent – depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds.*

8.1.6 Red Flag Indicators Related To Transaction Patterns

The red flags below illustrate how the misuse of VAs for ML/TF purposes could be identified through irregular, unusual, or uncommon patterns of transactions.

8.1.6.1 Transactions concerning new users

a. *Conducting a large initial deposit to open a new relationship with a VASP, while the amount funded is inconsistent with the customer profile;*
b. *Conducting a large initial deposit to open a new relationship with a VASP and funding the entire deposit the first day it is opened, and that the customer starts to trade the total amount or a large portion of the amount on that same day or the day*

after, or if the customer withdraws the whole amount the day after. As most VAs have a transactional limit for deposits, laundering in large amounts could also be done through over-the-counter-trading; and

c. *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.*

8.1.6.2 Transactions concerning all users

a. *Transactions involving the use of multiple VAs, or multiple accounts, with no logical business explanation;*
b. *Making frequent transfers in a certain period of time (e.g. a day, a week, a month, etc.) to the same VA account –*
    - ✓ *by more than one person;*
    - ✓ *from the same IP address by one or more persons; or*
    - ✓ *concerning large amounts.*
c. *Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency. Such transactions by a number of related accumulating accounts may initially use VAs instead of fiat currency;*
d. *Conducting VA-fiat currency exchange at a potential loss (e.g. when the value of VA is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical business explanation); and*
e. *Converting a large amount of fiat currency into VAs, or a large amount of one type of VA into other types of VAs, with no logical business explanation.*

8.2 Role of Key Partners/Stakeholders

The provision of some services in the sector may require inputs or responsibilities undertaken by third parties, counter parties, partners or stakeholders of the VASP. If such relationships/partnerships exists, the VASP has to ensure that such partners or

stakeholders have the operational, technical capacity and are willing to do their part in managing risks as per the FIA.

8.3 Type, Nature and Extent of Controls

The aim of managing risks in business is to reduce inherent[11] risks to tolerable or acceptable residual[12] levels. VASPs have a responsibility to implement controls and duly demonstrate their effectiveness to authorities such as the FIC. The FIC must be satisfied, upon such presentation, that such residual risk levels are tolerable or acceptable to the national AML/CFT/CPF framework. The entirety of controls, aligned to risks, should be documented in an AML/CFT/CPF Program or Policy document which needs management approval.

8.4 External Risk Assessments

The considerations and indicators herein are not exhaustive. VASPs are required to consider observations from SRA and NRA reports issued by the FIC. Local[13] and international trends and typology reports issued by bodies such as ESAAMLG[14] and FATF[15] (available on their websites), equally help highlight changing risks broadly and related to the sector. To the extent possible, this guidance has incorporated lessons and best practices from some local and international publications. ML and TF trends are dynamic, it is thus essential to keep abreast of updated publications in this regard.

8.5 Risk Assessment/Management Reports

All identified risks as far as clients, transactions and geographic considerations are concerned should be documented in Risk Management Reports. Such report(s)

[11] Inherent risks refer to the level of (original) risks prior to the implementation of controls to reduce the likelihood and impact of such risks.
[12] The remaining risk level after due controls have been implemented.
[13] Published on the FIC website under Risk Assessments folder while trends and typology reports are under Publications folder.
[14] https://www.esaamlg.org/index.php/methods_trends
[15] https://www.fatf-gafi.org/en/publications.html

(assessment outcomes) should be periodically updated when material changes arise in risks and controls.

9. FURTHER GUIDANCE ON CONTROLS

This Guidance Note deals with risk assessments as a foundational step for the implementation of an effective Risk Based Framework within VASPs. VASPs are further required to duly study Guidance Note 11 of 2023, amongst others, which speaks to the practical implementation of controls to mitigate ML/TF/PF risks at institutional level.

The FIC website contains several other Directives, Guidance Notes, Circulars and Regulations which avail helpful guidance on measures to combat ML/TF/PF in terms of the FIA.

10. GENERAL

This document may contain statements of policy which reflect the FIC's administration of the legislation in carrying out its statutory functions. This guidance is issued without prejudice to the FIA and its complementing Regulations. The information contained in this document is intended to only provide a summary on these matters and is not intended to be comprehensive.

11. NON-COMPLIANCE WITH THIS GUIDANCE

This document is a guide. Effective implementation is the sole responsibility of VASPs. Should an institution fail to adhere to the guidance provided herein, it will be such institution's responsibility to demonstrate alternative risk management controls implemented which are deemed effective by the FIC as supervisory authority implementing the FIA.

The Guidance Note can be accessed at www.fic.na

DATE ISSUED: 30 JUNE 2023

DIRECTOR: FINANCIAL INTELLIGENCE CENTRE

FIC CONTACT DETAILS

All correspondence and enquiries must be directed to:

The Director, Financial Intelligence Centre

P.O. Box 2882

No. 71 Robert Mugabe Avenue, Windhoek

helpdesk@fic.na

ANNEXURE A

GENERAL INDICATORS[16] IMPACTING ML/TF RISKS

a. Risk levels of different types of legal persons and arrangements: *The ability for criminals to hide their identity behind complex legal structures when conducting commercial transactions remains an attractive characteristic of legal persons and such other arrangements for ML/TF/PF purposes. Below are results from the 2023 NRA update showing how ML threats exploited various legal persons and trusts.*

CASES REFERRED FOR FURTHER INVESTIGATIONS: PERIOD: 2009 - 2021				
	Total STRs Received	**No. of Cases (SDs)**	**Total Financial Value from such Cases/SDs (NAD)**	**Average Financial value Per Case (NAD)**
Close Corporations (CCs)	228	104	34,807,766,160.75	334,690,059
Companies	232	115	8,659,067,618.13	75,296,240
Trusts	96	55	1,613,992,815.33	29,345,323
Natural Persons	5,690	1,696	23,404,719,080.81	13,799,952

b. Vulnerabilities with CCs: *The 2023 NRA update suggests that CCs are* ***the most abused type of legal persons*** *in terms of financial values[17]. This observation suggests that large scale ML in terms of financial values or impact is more likely to be advanced through CCs and to a lesser extent through companies and trusts.*

CASES REFERED FOR INVESTIGATIONS, PER PREDICATE OFFENCE: PERIOD: 2009 – 2021

[16] FIC Observations and risk assessments
[17] As per cases analysed by the FIC and referred to various investigative authorities on findings that suggest possible ML.

	Fraud	Total Financial Value (NAD)	Potential Tax Evasion	Total Financial Value (NAD)	Corruption	Total Financial Value (NAD)
Close Corporations (CCs)	25	404,533,140	66	28,400,797,080	7	394,575,890
Companies	56	656,836,151	141	738,080,077	35	284,419,187
Trusts	3	14,016,585	7	776,270,899	6	56,516,585
Natural Persons	667	1,695,855,636	2264	15,632,296,444	84	1,955,490,671

The high number of natural persons possibly implicated in ML activities still suggests that, by and large, people advance ML activities in their individual capacities, if the 2023 NRA update findings are anything to go by. Some STRs/SARs within the FIC suggests higher risks arise when there is a suspected use of personal funds for business purposes, or vice-versa.

c. Vulnerabilities with trusts: *In Namibian, a trust can either be a private trust or a public charitable trust. The 2023 NRA update suggests only inter-vivo trusts[18] may have been abused in advancing ML will all of them being (100%) Namibian initiated or founded (owned). None such trusts in ML or related predicate offence investigations are charitable trusts. The NRA further found that about 82% of these trusts have Namibian donors and Namibian trustees. Only 40% of the trusts involved in potential ML cases have foreign nationals listed as beneficiaries, with the majority being South African citizens.*

[18] Trusts created between living persons registered under the Trust Moneys Protection Act 34 of 1934.