Republic of Malawi

VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING RISK ASSESSMENT REPORT

June 2025

CONTENTS

DEFINITIONS ii
ACRONYMS iv
FOREWORD v
..... v
EXECUTIVE SUMMARY vi
1.0 INTRODUCTION 1
2.0 METHODOLOGY 3
3.0 THE VIRTUAL ASSET ECOSYSTEM IN MALAWI 8
4.0 RISK ASSESSMENT SURVEY RESPONSES 13
5.0 VIRTUAL ASSETS THREAT ASSESSMENTS 17
6.0 VIRTUAL ASSET INHERENT VULNERABILITY ASSESSMENT 24
7.0 MITIGATION MEASURES FOR VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 29
8.0 OVERALL COUNTRY RISK 31
9.0 CONCLUSION AND RECOMMENDATIONS 33
10.0 APPENDICES 34
11.0 REFERENCES 43

DEFINITIONS

Bitcoin (BTC)	The largest known cryptocurrency/virtual asset.
Blockchain	A complete ledger of transactions held simultaneously by multiple nodes on a network.
Centralised Exchange	A type of cryptocurrency exchange operated by a company that owns it in a centralised manner.
Cold Wallet	An offline wallet that is not connected to the internet and may include hardware, USB, and paper wallets.
Cryptocurrency	A digital asset can be used as a store of value or a medium of exchange for goods and services. Transactions are verified and recorded using cryptography by a distributed network of participants rather than a centralised authority such as a bank or government agency.
Custodial Wallet	An online virtual asset wallet that stores VAs on behalf of a VA owner and does not provide full control of VAs.
Dark Web	The part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.
Decentralised Exchange	P2P trading platform enables users to exchange cryptocurrencies without relying on a central intermediary or custodian.
Fiat Currency	Currencies with legal tender, such as, the Malawi Kwacha, the U.S. dollar, the Euro or the British pound, are examples of fiat currencies.
Fiat-to-Virtual	The conversion of government issued fiat currency to VAs.
Hot Wallet	A tool that allows users to store, send, and receive tokens. They are linked with public and private keys that help facilitate transactions and act as a security measure.
Mining	The process that generates new VAs and verifies new transactions.
Non-Custodial Wallet	A virtual asset wallet that stores VAs and enables VA owners to have full control of their VAs and can be a program or a physical device.
Peer-to-Peer	A form of virtual asset exchange that entails the transfer of virtual assets from one user to another.

Stablecoin	A virtual asset that aims to maintain a stable value relative to a specific asset or a pool or basket of asset to reduce volatility.
Traditional Obligated Entities	Refer to all reporting institutions that are required to comply with AML/CFT/CFP obligations and comprise Financial Institutions and Designated Non-Financial Businesses and Professions.
Virtual Asset	A digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes.
Virtual Asset Exchanges	An online platform that facilitates virtual asset transfers and exchanges. Exchanges may occur between one or more forms of virtual assets, or between virtual assets and fiat currency.
Virtual Asset Investment Providers	The practice of providing an investment vehicle enabling investment in/ purchase of VAs via a managed investment scheme.
Virtual Asset Service Provider	Any natural or legal person that conducts the following activities or operations for or on behalf of another natural or legal person: a. Exchange between virtual assets and fiat currencies; b. Exchange between one or more forms of virtual assets; c. Transfer of virtual assets; d. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and e. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
Virtual Asset Wallet	A program or device that stores VAs.
Virtual Asset Wallet Providers	Persons that provide storage for virtual assets or fiat currency on behalf of others.
Virtual-to-Fiat	Conversion of VAs to fiat currencies.
Virtual-to-Virtual	Conversion of one type of VA to another
Wallet	A digital storage device or location for keeping crypto assets secure.

ACRONYMS

AML/CFT/CFP	Anti-Money Laundering / Countering the Financing of Terrorism and Proliferation
AEC	Anonymity Enhanced Cryptocurrency
CDD	Customer Due Diligence
DNFBPs	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FIA	Financial Intelligence Authority
FIs	Financial Institutions
KYC	Know Your Customer
LEA	Law Enforcement Agency
ML/TF/PF	Money Laundering/Terrorist Financing/Proliferation Financing
P2P	Peer to Peer Transactions
P2B	Peer to Business Transactions
RBM	Reserve Bank of Malawi
TOE	Traditional Obligated Entities
TWG	Technical Working Group
VA	Virtual Asset
VASP	Virtual Asset Service Provider

FOREWORD

The Government of Malawi remains fully committed to upholding the integrity and resilience of its financial system in the face of evolving global risks. In line with this commitment, and in accordance with the Financial Action Task Force (FATF) Standards, Malawi undertook the first risk assessment of Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs). This assessment forms a critical component of our broader strategy to strengthen the national framework for combating money laundering, terrorist financing and proliferation financing (ML/TF/PF).

The rise of VAs and the rapid development of associated technologies enabling their transfer and storage have introduced significant opportunities for innovation and financial inclusion. However, these advancements carry substantial risks, particularly due to the anonymity, speed, and cross-border nature of VA transactions, which can be exploited by criminals to conceal and move dirty funds without detection.

Recognizing these dynamics, FATF enhanced the requirements of Recommendation 15 on new technologies for jurisdictions to identify, assess, and understand risks associated with VAs and VASPs and apply risk-based measures. Malawi's decision to conduct the sectoral risk assessment is, therefore, not only a fulfilment of international obligations but also a proactive step to safeguard our financial system from emerging ML/TF/PF threats. Through this process, the Government seeks to ensure that any identified threats and vulnerabilities are urgently addressed and that the benefits of VAs are responsibly harnessed. The assessment findings shall inform Malawi's policy stance on the treatment of VAs and VASPs and guide establishment of a relevant legislative environment for VAs and VASPs in Malawi.

I wish to commend all institutions and stakeholders who contributed to this important initiative. Particularly, I extend my sincere appreciation to members of the Risk Assessment Technical Working Group, which drew representation from, among others, the Reserve Bank of Malawi, the Financial Intelligence Authority, and the Ministry of Finance and Economic Affairs, for the dedication and professionalism exhibited towards successful completion of the exercise. Their collective efforts have established a strong foundation for a more secure, transparent, and resilient digital financial ecosystem. As we move forward, the Government remains steadfast in its commitment to fostering a sound, safe and inclusive financial sector that drives sustainable economic growth while safeguarding the public against financial crimes.

Honourable Simplex Chithyola Banda, MP.

MINISTER OF FINANCE AND ECONOMIC AFFAIRS

EXECUTIVE SUMMARY

The Government of Malawi, in alignment with its commitment to uphold the integrity of the financial system and adhere to international standards, has conducted the first money laundering, terrorism financing and proliferation financing (ML/TF/PF) risk assessment for VAs and VASPs. This initiative was undertaken in response to the evolving global digital financial landscape and compliance with the requirements of FATF Recommendation 15, which calls on jurisdictions to identify, assess, and mitigate risks related to VAs and VASPs.

Key Assessment Outcomes:

1. **High national ML/TF/PF risk exposure:** The overall exposure of Malawi to ML/TF/PF risks stemming from VAs and VASPs is rated **high**. This is primarily due to elevated levels of inherent threats and sector vulnerabilities, as well as low effectiveness controls;
2. **High-risk channels and products:** The assessment identified P2P transactions, custodial wallet services, and cross-border platform operations as posing high risks as they present anonymity, traceability, and enforcement challenges;
3. **Regulatory and supervisory gaps:** Malawi currently lacks a dedicated legal and regulatory framework to govern VA and VASP activities. This regulatory and supervisory vacuum presents significant risks, as VASPs operate without licencing, oversight, and enforcement regimes;
4. **Emerging use and unregulated ecosystem:** While the regulated sector's engagement remains limited, the risk assessment affirmed the growing public use of VAs for multiple purposes, including savings, investments, and cross-border transfers. Unlicensed/unregistered and foreign-based VASPs are increasingly entering the local market and operating without any regulatory scrutiny; and
5. **Institutional capacity constraints:** Regulatory and supervisory authorities, law enforcement agencies (LEAs), and other competent authorities have demonstrated limited capacity to identify, monitor, and investigate VA-related financial crime, hindering effective risk mitigation and enforcement. This may weaken the country's financial system integrity and expose Malawi to potentially high and unmonitored ML/TF/PF risks.

Strategic Remedial Measures:

To address the elevated risk exposures and close critical regulatory and institutional gaps, the following actions are recommended:

a) **Define a clear policy stance:** Malawi should define a clear policy stance on allowing or prohibiting VAs and VASPs and ensure a relevant legislative environment on their treatment;
b) **Strengthen institutional capacity:** The county needs to build technical capabilities across key government institutions, including regulatory and supervisory authorities,

LEAs, and other relevant authorities, to enhance detection, investigation, monitoring, and enforcement capabilities;

c) **Enhance coordination and information sharing:** The country needs to facilitate inter-agency collaboration and establish protocols for international cooperation to counter the cross-border nature of VA-related threats and curb illegal VASPs' operations; and

d) **Promote public awareness and stakeholder engagement:** This can be achieved through financial literacy and targeted awareness programs aimed at informing the general public and the private sector about risks and obligations associated with VA usage.

The risk assessment is a critical step in safeguarding Malawi's financial system from the evolving risks associated with VAs and VASPs. The findings underscore the urgent need for coordinated policy and regulatory intervention to ensure that innovation in the financial sector does not compromise national security and financial stability. The country's proactiveness in addressing the identified risks will be essential to fostering a secure, transparent, and resilient digital financial environment that supports inclusive economic growth, while effectively dealing with ML/TF/PF threats.

1.0 INTRODUCTION

1.1 Background

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. VAs do not include digital representation of fiat currencies, securities and other financial assets. Examples of VAs include Bitcoin, Ethereum, Solana, Ripple and Stablecoins, including USDT.

Further, FATF defines a virtual asset service provider as any natural or legal person that conducts the following activities or operations for or on behalf of another natural or legal person:

a. Exchange between virtual assets and fiat currencies.
b. Exchange between one or more forms of virtual assets.
c. Transfer of virtual assets.
d. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
e. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

There is rapid growth and adoption of VAs and VASPs globally and across Sub-Saharan Africa, with over 500 million users[1] and over 6,000 registered VASPs[2] processing an estimated USD5.7 trillion globally and USD125 billion cryptocurrency value in Sub-Saharan Africa, respectively, as of July 2024. Specifically, in Sub-Saharan Africa's crypto economy, stablecoins have become a key element in countries where local currencies are highly volatile and access to US dollars is limited. Dollar-pegged stablecoins like USDT and USDC have gained traction, offering businesses and individuals alike a reliable way to store value, facilitate international payments, and support cross-border trade. Stablecoins now account for approximately 43 percent of the region's total transaction volume[3]. The trend has introduced both opportunities and significant financial crimes risks to the financial systems of developing and developed economies alike.

In Malawi, the increasing interest in VAs is largely driven by their accessibility, speed, low transaction costs, and borderless nature of use. Individuals, including students, professionals, and entrepreneurs, are increasingly utilising VAs for various purposes, including savings, investments, remittances, and online payments. On the other hand, VAs and VASPs are vulnerable to potential misuse for ML/TF/PF. The VA sector poses complex and novel threats to a country's efforts to deter financial crime. The pseudo-anonymous nature of many VA transactions allows illicit actors to exploit them to obscure the origins of illicit and/or licit

[1] https://www.triple-a.io/cryptocurrency-ownership-data
[2] https://coincub.com/vasp-registration-report-2024-coincub/
[3] The 2024 Geography of Crypto Report

proceeds, making detection, investigation, and prosecution by competent authorities significantly more challenging. Recognizing the evolving threats, the FATF revised standards to explicitly extend AML/CFT/CFP obligations in relation to VAs and VASPs in 2019. In this regard, the FATF requires countries to identify, assess, and understand the ML/TF risks associated with new technologies, including VAs and the entities facilitating their exchange, safekeeping, or investment (VASPs). The requirements were introduced immediately after Malawi's mutual evaluation exercise. Until now, the country has no market entry and AML/CFT/CFP legislation applicable to the VA ecosystem.

In alignment with the international obligations and building upon the recommendations of the 2019 Malawi Mutual Evaluation Report by the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), the country has undertaken the first sectoral risk assessment focusing on VAs and VASPs. All the previous National Risk Assessments (NRAs) did not cover the sector.

The assessment was guided by the FATF Standards and the World Bank's VAs and VASPs ML/TF Risk Assessment Tool. Data and information were drawn from government institutions, financial sector regulators, law enforcement agencies, private sector reporting entities, the general public, and open sources. In addition, the assessment reviewed similar studies from some African jurisdictions and other countries across the globe; including Kenya, Guyana, Jordan, Seychelles, Mauritius, and Singapore.

1.2 Objectives

The primary objective of the risk assessment was to identify, evaluate and understand ML/TF/PF risks to inform a policy stance on regulation and supervision of VAs and VASPs in Malawi.

Specifically, the assessment sought to:

i. Identify, understand and assess the overall money laundering and terrorist financing (ML/TF/PF) risks related to the VA and VASP sector;
ii. Identify VA and the VASP products/services/channels with high vulnerability;
iii. Prioritise action plans to strengthen anti-money laundering and combating the financing of terrorism and proliferation (AML/CTF/CFP) measures in the VA and VASP sector; and
iv. Identify capacity gaps among law enforcement authorities, supervisory authorities, and other relevant authorities.

2.0 METHODOLOGY

2.1 Technical Working Group

To conduct the sectoral VAs/VASPs ML/TF/PF risk assessment, a Technical Working Group (TWG) was instituted. The TWG comprised financial sector regulators, LEAs and relevant government Ministries namely:

i. Ministry of Finance and Economic Affairs;
ii. Reserve Bank of Malawi (RBM);
iii. Financial Intelligence Authority (FIA);
iv. Ministry of Justice;
v. Law Enforcement Agencies; and
vi. Malawi Gaming & Lotteries Authority (MAGLA).

2.2 Scope of the Risk Assessment

The scope of the assessment was mainly informed by the World Bank's National Risk Assessment Tool for VA & VASPs (World Bank Tool) and the FATF's guidance on risk-based approach to VAs and VASPs. To better comprehend the Malawian VA and VASP ecosystem, the TWG undertook the following:

i. Identified the VAs and VASPs in Malawi eco-system and how they interact with TOEs;
ii. Identified the potential VA/VASP threats and their impact on ML/TF/PF;
iii. Identified the potential VA/VASP vulnerabilities that could be exploited for ML/TF/PF;
iv. Assigned a risk level to each identified vulnerability and threat;
v. Identified existing controls put in place to mitigate each identified risk; and
vi. Proposed recommendations to effectively mitigate the identified ML/TF/PF risks.

2.3 The Risk Assessment Tool

The World Bank Tool identifies seven types of VASPs, 12 services of VASPs, and 27 activities/channels with distinct assessment criteria for each product, service or activity. Table 1 below summarises key components of the World Bank Tool:-

Table 1: Key Components of the World Bank NRA Tool

TYPE OF VASP	VASP SERVICE	VA CHANNEL
Virtual Asset Wallet Providers	Custodial Services	- Hot Wallet
	Non-Custodial Services	- 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	Fund Management	-
	Fund Distribution	-
	Compliance, Audit and Risk Management	-
Initial Coin Offering (ICO) Providers	Fund Raising	- Fiat-to-Virtual
		- Virtual-to-Virtual
	Investment	- Development of Product & Services
	Other Offerings	- Security Token Offerings (STOs)
		- Initial Exchange Offerings (IEOs)
Virtual Asset Investment Providers	Trading Platforms	- Platform Operators
		- Custody of Assets
		- Investment into VA-related commercial activities
		- Non-Security Tokens & Hybrid Trading Activities
		- Stablecoins
	Emerging Products	- Crypto Escrow service
		- Crypto-custodian Services
Validators/Miners/Administrators	Proof of Work	- Fees
		- New Assets

Source: The World Bank

2.4 FATF Guidance and Recommendations on VAs and VASPs

The TWG considered FATF guidance and Recommendations relating to VAs and VASPs in conducting the risk assessment. In 2019, the FATF extended AML/CFT standards to VAs and VASPs to prevent criminal and terrorist misuse of the sector. In October 2021, it updated the 2019 guidance for a risk-based approach to VAs and VASPs.

The Guidance examines how VA activities and VASPs fall within the scope of the FATF Standards. It discusses the five types of activities covered by the VASP definition and provides examples of VA-related activities that would fall within the definition and those that would potentially be excluded from the FATF scope. In that respect, it highlights the key elements required to qualify as a VASP, namely acting as a business for or on behalf of another person and providing or actively facilitating VA-related activities.

The Guidance outlines the need for countries, VASPs, and other entities involved in VA activities to understand ML/TF risks associated with VA activities and take appropriate mitigating measures to address those risks. In particular, the Guidance provides examples of risk indicators that should specifically be considered in a VA context, with an emphasis on factors that would further obfuscate transactions or inhibit VASPs' ability to identify customers.

The Guidance highlights the VASP registration or licencing requirements and how to determine the appropriate VASP registration or licencing jurisdiction – at a minimum, where they were created or in the jurisdiction where their business is, in cases where they are natural persons. However, jurisdictions can also choose to require VASPs to be licensed or registered before conducting business in or from their jurisdiction. The Guidance further underlines that national authorities are required to take action to identify natural or legal persons that carry out VA activities without the requisite license or registration.

Regarding VASP supervision, the Guidance makes it clear that only competent authorities, and not self-regulatory bodies, can act as VASP supervisory or monitoring bodies. They should conduct risk-based supervision or monitoring and have adequate powers, including to conduct inspections, compel the production of information and impose sanctions. There is a specific focus on the importance of international cooperation between supervisors, given the cross-border nature of VASPs' activities and provision of services.

2.5 Data Collection Tools and Analysis

In undertaking the risk assessment, the TWG employed two main methods of collecting qualitative and quantitative data about VAs and VASPs. These were:

a) Survey questionnaires; and
b) Review of documents and other literature from open sources such as reports of international standard-setting bodies, reports of regulatory authorities, and relevant Government reports.

Questionnaires were administered to multiple stakeholders, including financial institutions (FIs), Designated Non-Financial Businesses and Professions (DNFBPs), supervisory authorities, LEAs, unlicensed/unregistered VASPs and the general public.

The questionnaire for FIs, DNFBPs and unlicensed/unregistered VASPs was designed to collect information on the extent of utilization of VAs and existence of VASPs in Malawi. The

questionnaire further assisted in determining whether FIs and other service providers understood and adopted adequate measures to mitigate ML/TF/PF risks.

The supervisory authorities' questionnaire aimed to understand the adequacy of regulatory measures and supervisory frameworks to address VA and VASP activities. It was also designed to establish whether supervisory authorities have the necessary power, skills, and resources to cover the specific areas relating to VASPs on a risk-based approach.

The LEA's questionnaire was designed to understand how the agencies comprehend the risks and adequately apply risk-based measures. It also collected information to establish whether LEAs have the necessary powers, skills, and resources to cover the specific areas relating to VASPs.

The public questionnaire sought to understand the public's use, knowledge, and perceptions of VAs and VASPs, including their understanding of risks.

A total of 262 responses to the survey questionnaires were received, as highlighted in Table 2 below. Data analysis was conducted with the aid of the World Bank Tool.

Table 2: Questionnaire Survey Response Summary

Respondent Category	Number of Responses
Public	188
FIs, DNFBPs, and Others	67
Law Enforcement Agencies	3
Supervisory Authorities	4
Total	**262**

2.6 Challenges and Limitations

In conducting the risk assessment, the following challenges were encountered:

i. Use of open data sources, whose accuracy required further verification; and
ii. Lack of information and data emanating from the fact that the VA sector is unregulated in Malawi.

Despite the challenges above, the sources of information, analyses and results of the risk assessment are broadly representative. In addition, the findings underwent a validation process during a meeting held on 26 June 2025 attended by various stakeholders which included supervisory authorities, LEAs, FIs, DNFBPs, unlicenced/unregulated VASP, relevant government ministries and agencies, academia such as students and Malawi University of Science and Technology, VA users, United Nations Capital Development Fund (UNCDF) and Finmark Trust, among others. The assessment can, therefore, be relied upon for use by all relevant stakeholders.

2.7 Presentation of Assessment Findings

As guided by the World Bank tool, the assessment established the overall ML/TF/PF risk by separately analysing threats and vulnerabilities of VAs and VASPs as well as levels of

effectiveness in mitigating identified risks. Threat assessment is covered under section 5.0, whereas section 6.0 discusses the vulnerabilities. Assessment of mitigating measures is discussed under section 7.0. The overall country ML/TF/PF risk is detailed in section 8.0.

3.0 THE VIRTUAL ASSET ECOSYSTEM IN MALAWI

This section details the VA landscape in Malawi and evaluates the interaction of VASPs with TOEs in the country.

3.1 The VA Landscape in Malawi

At the time of the assessment, Malawi did not have any legislative regime to regulate and supervise VASPs. The assessment, however, confirmed the existence of VA activities and VASPs operations in the country. One entity had physical presence and existed as an unlicensed/unregistered VASP (offering currency exchange and Bitcoin), whereas 11 firms were providing online platforms[4] where users are onboarded on VA wallets and exchanges and access investment services[5]. For the year ending April 2025, the VASP with physical presence registered over 84,000 customers with transaction volumes amounting to USD 2.4 million[6]. The sector also had some organisations, academia and students undertaking various VA-related activities, including mining, research, and awareness. In view of the VA ecosystem in Malawi, the TWG assessed three types of VASPs, five services and eight channels as detailed in Table 3 below: -

Table 3: Types of VASPs and their Services

Type of VASP	Type of Service	Channel
Virtual Asset Wallet Providers	Custodial Services	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 Investment Providers	Trading Platforms	Platform Operators

3.2 Interaction with Traditional Obligated Entities[7]

The interaction of VASPs and TOEs, such as banks and other entities, is critical in the broader financial ecosystem. As VASPs increasingly integrate with conventional financial channels for fiat-to-virtual, virtual-to-fiat, or related conversion services, their relationship with TOEs raises new AML/CFT/CFP compliance challenges. These interactions can expose and facilitate ML/TF/PF activities if appropriate customer due diligence measures are not enforced.

[4] 6 VASPs were confirmed through survey responses from the general public while 5 (Bitget, Rexl, Mama Exchange, Bit Mama and Shifu Pay) were identified from open sources.
[5] RBM has been receiving some applications for formal licensing of VASPs in Malawi.
[6] Yellow Card Financial
[7] Indicated figures as at December 2023 (The Registrar of Financial Institutions 2023 Annual Report)

Therefore, the assessment analysed the nature of interactions between the VA sector and key TOEs, including banks, mobile money operators and DNFBPs.

3.2.1 Banking Sector

Malawi's banking sector consisted of eight commercial banks, which are divided into four domestically owned and four foreign-owned institutions. Among these, four banks are publicly traded on the Malawi Stock Exchange, and all are licensed and supervised by the RBM, acting as the Registrar of Financial Institutions. The sector plays a significant role in the financial system, serving as the primary channel for capital flows, payments, and investments. Banks are governed by prudential regulations under the Financial Services Act and the Banking Act. Additionally, the RBM fulfils the role of supervisor for AML/CFT/CFP regulations, working alongside the FIA to enforce the Financial Crimes Act and subsidiary legislation. Compliance is ensured through risk-based supervision, transaction monitoring, and adherence to KYC/CDD and reporting requirements.

The interaction between banks and VASPs in Malawi was limited and largely indirect. Banks process incoming and outgoing transfers related to VASP activity primarily through traditional instruments such as bank transfers and card payments. The transactions were processed within the existing banking framework and are subject to AML/CFT/CFP oversight.

In the absence of legal provisions preventing dealing in VAs or engaging directly with VASPs, banks adopted a conservative stance. None of the banks engaged in proprietary trading of VA nor confirmed direct dealings with VASPs. However, from supervisory sources, the assessment established that some banks provide direct banking services to VASPs, such as accounts and cards. This was further confirmed by the general public in responses to the risk assessment survey. Customer-initiated transactions to VASPs are mostly routed through P2P mechanisms or card rails, which are subject to daily and per-transaction limits. According to the responses, this cautious approach was driven by the absence of clear regulatory frameworks, concerns over the evolving nature of VAs, and the complex legal and corporate structure for VASPs.

3.2.2 Microfinance Sector

The Microfinance sector comprised five deposit-taking, 13 non-deposit-taking, over 70 micro-credit agencies, and 34 financial cooperatives. The sector was governed by, among others, the Financial Services Act, Microfinance Act, Financial Cooperatives Act, Financial Crimes Act, and subsidiary laws, guidelines and directives. All the institutions were under prudential, non-prudential, and AML/CFT/CFP risk-based supervision by the RBM. No firm in the sector confirmed to have any interaction with the VA ecosystem.

3.2.3 Pension and Insurance Sector

The pension sector comprised five pension service companies, five pension brokers, 19 stand-alone pension funds, two self-administered pension funds, nine unrestricted pension funds, two umbrella schemes, one voluntary pension fund and one provident fund. The sector was primarily governed by, among others, the Financial Services Act, Pensions Act and subsidiary laws.

On the other hand, the insurance sector had eight general insurance companies, six life insurance companies, one reinsurance entity, one reinsurance broker, 21 insurance brokers, and multiple insurance agents. The sector was mainly governed by the Financial Services Act, Insurance Act, Financial Crimes Act and subsidiary laws.

All the institutions in the sector were under prudential and AML/CFT/CFP risk-based supervision by the RBM, and none of the entities confirmed to have directly or indirectly interacted with the VAs or VASPs.

3.2.4 Capital Market Sector

The capital markets comprised one stock exchange, two collective investment schemes, 12 investment advisers, three brokers, three transfer secretaries, and six portfolio managers. Malawi's capital market players are governed by a robust legislative framework, including the Financial Services Act, Securities Act, and Financial Crimes Act. All the entities are under prudential and AML/CFT/CFP risk-based supervision by the RBM.

Market players in the sector indicated that they do not deal in VAs or directly/indirectly interact with VASPs. However, one portfolio manager confirmed to have some knowledge and expertise in VA and only offers investment advice to its customers seeking to diversify their portfolios.

3.2.5 Payment Sector

Malawi's payment sector was governed by the Payment Systems Act and constituted seven electronic money issuers, four payment aggregators, two payment gateways, and two payment system operators. The RBM provided regulatory oversight for the sector, ensuring the safety, efficiency, and integrity of payment systems. The FIA provided AML/CFT/CFP oversight across all system operators.

Mobile money had significantly improved financial inclusion in Malawi, especially in rural areas, serving as a low-barrier entry point into the formal financial system. In Malawi, electronic money wallets were a key funding source for customers interacting with VASPs. Customers were initiating transfers from their wallets to platforms, allowing the acquisition of VAs. The transactions were typically passed through regulated payment gateways, providing a degree of oversight and traceability and were subjected to Know Your Customer (KYC) and transactional thresholds enforced by both the VASPs and electronic money issuers. However, the regulatory boundary became unclear once customers transfer their funds to VASPs or external wallets, especially when engaging with cross-border or unregulated platforms.

There was no evidence of payment sector players interacting with high-risk foreign VASPs or decentralised exchanges. Nevertheless, responses from the general public affirmed that some users of local VASPs transfer VA assets to unregulated external wallets, raising concerns about potential exposure to illicit finance or loss of funds.

3.2.6 Designated Non-Financial Businesses and Professions

Malawi's DNFBPs comprised casinos, lawyers, real estate agents, accountants and dealers in precious metals and stones. The country had five casinos, two Wide Area Progressive gaming licensees, two gaming machine operators, and 10 sports betting operators. MAGLA was the supervisory authority responsible for licencing, registration and AML/CFT/CFP supervision. In addition, there were 41 licenced and 259 unlicensed real estate businesses and operators. The Lands Economy Board was responsible for licencing and the FIA for AML/CFT/CFP supervision. Further, the mining sector had 32 groups of informal ASM operators, with 17 having undergone a full formalization process. The Mining and Minerals Authority was responsible for licencing, while the FIA was responsible for AML/CFT/CFP supervision.

For lawyers, there were 188 licenced legal firms and 770 legal practitioners, and the Malawi Law Society was responsible for licencing. On the other hand, there were 43 registered accountancy and audit firms and 90 practising certified public accountants. The Malawi Accountants Board was responsible for licencing and the FIA for AML/CFT/CFP supervision of both professions.

Generally, the DNFBPs had little understanding of the risks they face and their AML/CFT/CFP obligations. Relatedly[8], the DNFBPs may have little awareness on the red flags associated with ML/TF/PF in the context of VAs. Globally, there was a growing trend for gaming platforms to accept digital currencies as a form of payment due to their ability to facilitate fast transactions, lower fees, increased privacy and reach.

The responses from the DNFBPs did not indicate their interaction with VASPs in manner or form. The absence of regulatory frameworks on VAs and VASPs in the country poses a challenge on how the DNFBPs should handle their interaction with VASPs. The responses by the public in Malawi that they are users of VAs was an indication that they could use them for various reasons, including online betting, payments or investments in the form of purchase of real estate and other assets. In this regard, gaming clients could have an emerging appetite for the use of digital currencies, especially in sports and online betting, given that this trend was growing internationally. The gaming sector only allowed cash, debit cards and mobile money as modes of payment.

Table 4 below indicates the extent of interaction between the VA sector and TOEs and the unregulated sector in Malawi.

[8] Malawi Mutual Evaluation Report 2019

Table 4: Sector Interaction with VA Channels

	Chanels	Banks	NBFI	Unregulated	Accountants	Legal Professionals	Casinos, Gaming & Betting	Real Estate Agents
VA Wallet Providers	Hot Wallet			●				
VA Exchanges	P2P			●				
	P2B			●				
	Fiat-to-Virtual	●	●	●				
	Virtual-to-Fiat	●		●				
	Virtual-to-Virtual			●				
VA Investment Providers	Platform Operators			●				

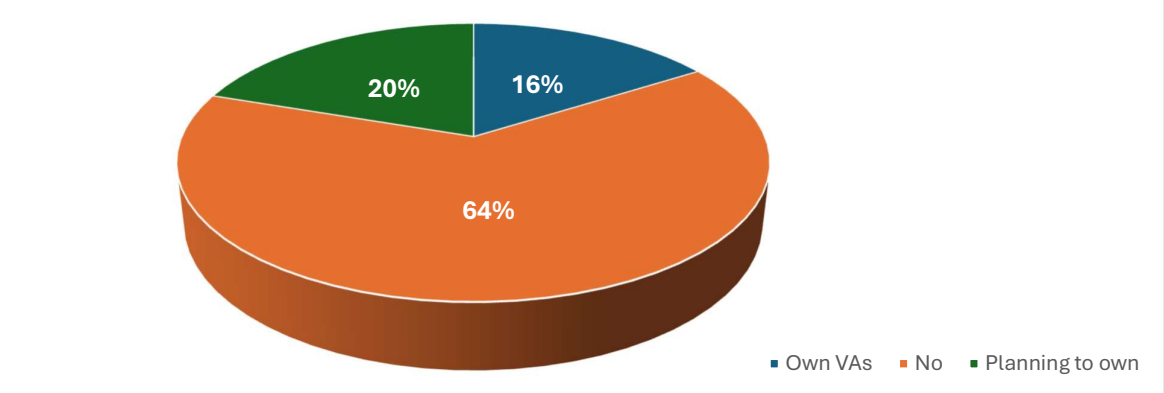
4.0 RISK ASSESSMENT SURVEY RESPONSES

This section highlights key responses from the survey questionnaire administered to the general public, supervisory authorities and LEAs.

4.1 Virtual Asset Usage

The survey showed that, out of 188 responses from the general public 16 percent owned VAs while 20 percent was planning to own. Figure 1 below indicates the rate of VA usage by the respondents: -

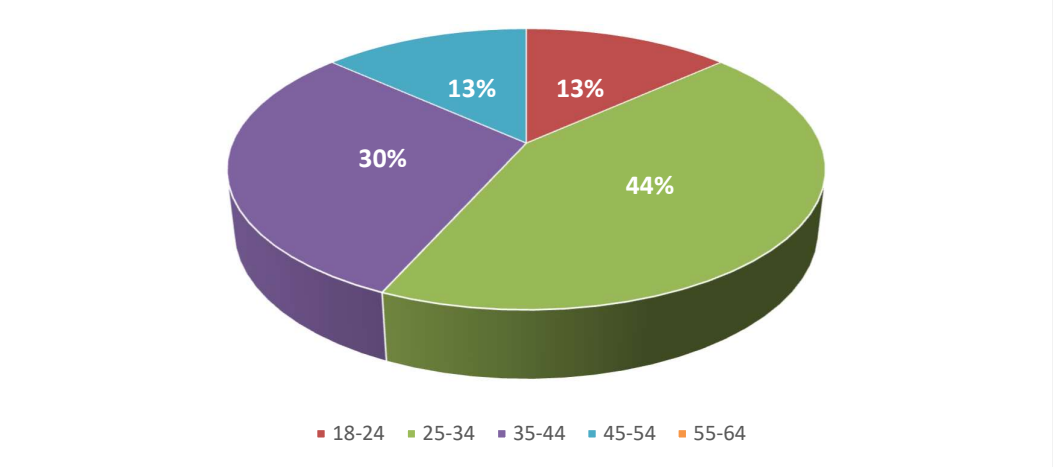
Figure 1: VA Usage by Respondents



4.2 Age Distribution of VA Users

The responses from the general public indicated that VA usage in Malawi is mostly associated with the youth, who were within the age brackets of 25-34 and 35-44. Figure 2 below depicts the age distribution for VA-user respondents: -

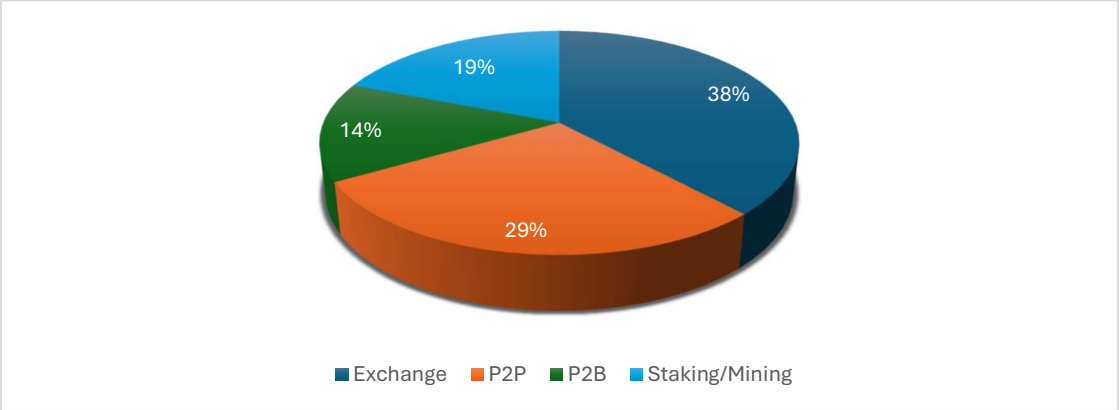
Figure 2: Age Distribution of Respondents



4.3 Means of Acquiring VAs

Majority of respondents, 38 percent, acquired VAs from the centralized exchanges, whereas 29 percent and 14 percent acquired their VAs through peer-to-peer and peer-to-business trading, respectively. Further, 19 percent acquired VAs through staking or mining. Figure 3 below depicts the means through which the respondents acquired VAs: -

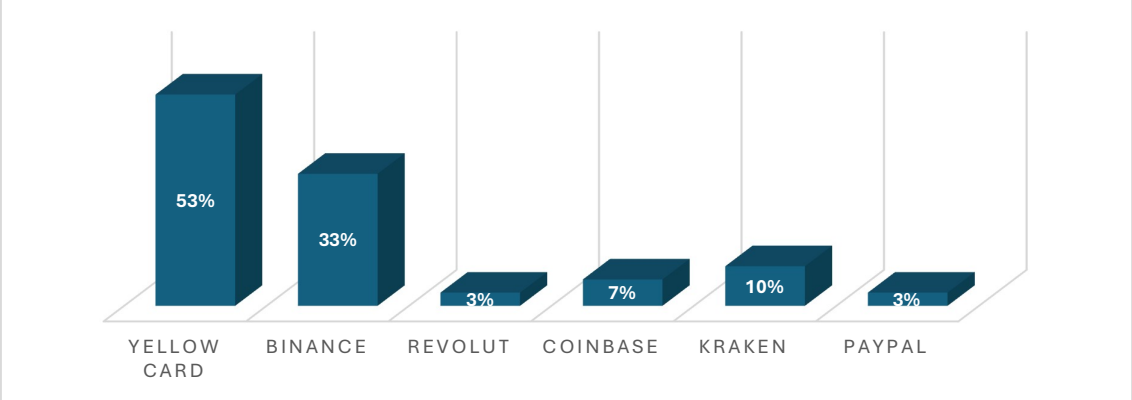
Figure 3: Means of Acquiring VAs by Users



4.4 VASPS Used by Respondents

Most respondents, representing 53 percent, utilised a locally available unlicensed/unregistered VASP (Yellow Card) to acquire VAs. The rest of the respondents utilised international based VASPs including Binance (33 percent) and Kraken (10 percent). Figure 4 below indicates some of the VASPs used by the respondents: -

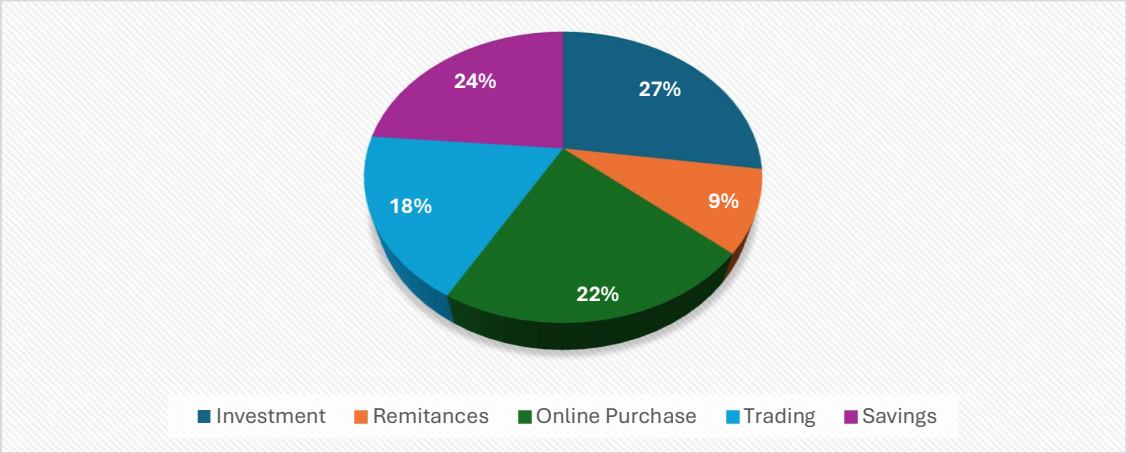
Figure 4: VASPs Used by Respondents



4.5 Primary Reasons for VA Usage

The survey revealed that 24 percent of users were utilising VAs for savings, 27 percent for investments and 22 percent online purchases as indicated in Figure 5 below: -

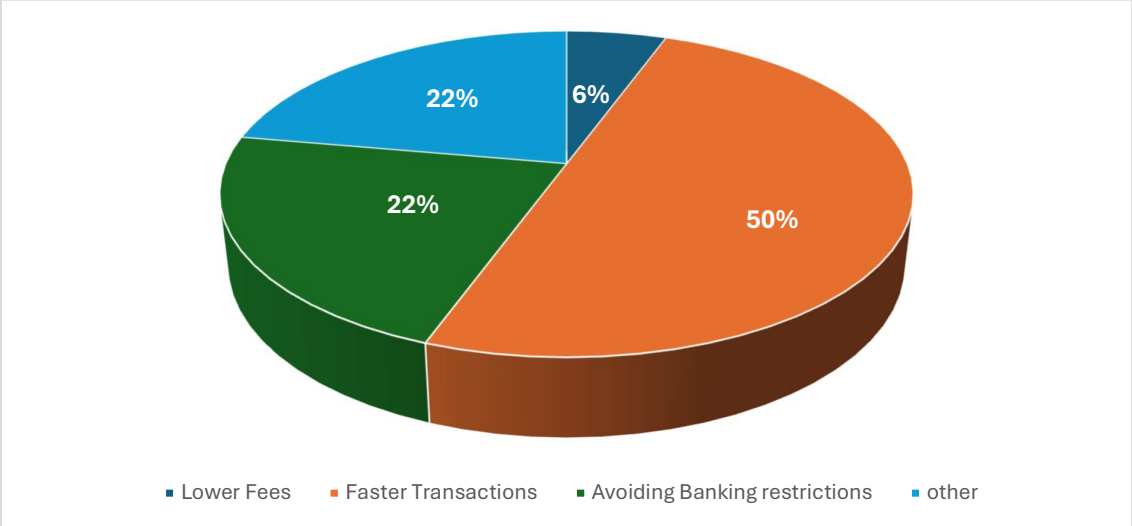
Figure 5: Reasons for VA usage by Users



4.6 Usage of VAs for Cross-Border Payments

The survey also showed that 40 percent of users were utilising VAs to process cross-border payments. Most users, 50 percent, were persuaded by speed of transactions, whereas 22 percent utilized the service to avoid perceived bank restrictions, the other 22 percent indicated other reasons including higher exchange rates when reselling the VAs and avoiding lengthy formal sector foreign exchange transactions approvals. Figure 6 below depicts reasons for utilizing VAs for cross border payments: -

Figure 6: Reasons for Utilizing VAs for Cross-Border Payments by Users



4.7 Involvement of FIs, DFBPS and Unregulated Sector in VA

The survey established that three institutions were involved in VA activities. Two of the institutions were from the unregulated sector and were offering VA exchange services and

education/awareness with much emphasis on Bitcoin investment. In addition, one licenced non-bank FI which was interacting with the VASPs in collecting and disbursing funds on behalf of the VASPs.

4.8 VASPS Supervision

The survey responses indicated that the country's supervisory authorities were not registering, licencing and supervising VASPs. Thus, supervisory authorities had no legal framework prescribing entry controls for VASPs and minimum AML/CFT regulatory provisions to be complied with by the VASPs. Further, the authorities indicated that they had limited knowledge on regulation, supervision and risks of the sector.

4.9 Investigations, Tracing and Seizure of VAs by Law Enforcement Agencies

The survey revealed limited understanding of risks and lack of capacity by all the country's LEAs to investigate, trace, prosecute, seize, and confiscate VAs and/or VASPs associated with illicit activities.

5.0 VIRTUAL ASSETS THREAT ASSESSMENTS

This section analyses threats from predicate offenses sourced from relevant Authorities and credible publications as well as those inherent in VAs and VASPs, as assessed utilising the Risk Assessment Tool.

5.1 Threat from ML Predicate Offenses

Based on the country's 2024 NRA findings, predicate offences that generate a significant amount of proceeds and pose ML threats are corruption, illegal externalisation of foreign currency, tax evasion and fraud. These offenses may affect the VA sector in Malawi in various ways, and the assessment identified three fraud cases as detailed below: -

Case 1: Crypto Currency Fraud in Malawi[9]

The Malawi Police Service arrested suspects in connection to Cryptocurrency Fraud that defrauded several individuals through a foreign based VASP. The suspects were to answer charges on operating a business as a financial institution without being registered or licensed; conspiracy to defraud; and fraud other than false pretence. The case involved 3 suspects who had defrauded victims more than K130 million.

Case 2: 'Disappearing VASPs'[10]

Another case involved a victim who placed funds in an alleged online VASP account, with the anticipation that the investment would double every fortnight. However, after a week, the victim could no longer trace the alleged VASP's website. The provider did not have physical presence in Malawi.

Case 3: 'Suspected Ponzi Scheme in Malawi'[11]

Several high-profile incidents have shed light on the severity of Bitcoin fraud in Malawi. For example, a Ponzi scheme promising quick returns through cryptocurrency investments defrauded many individuals of their savings. Additionally, there have been instances of ransomware attacks targeting businesses and individuals, demanding Bitcoin payments in exchange for unlocking encrypted data.

[11] Wiki Crypto News - Legal Perspectives on Fraudulent Bitcoin Activities in Malawi

Considering the nature and complexity of VAs and VASPs operations, and absence of regulation and supervision for the sector, it is possible that some VA users did not report any cases involving more predicate offenses.

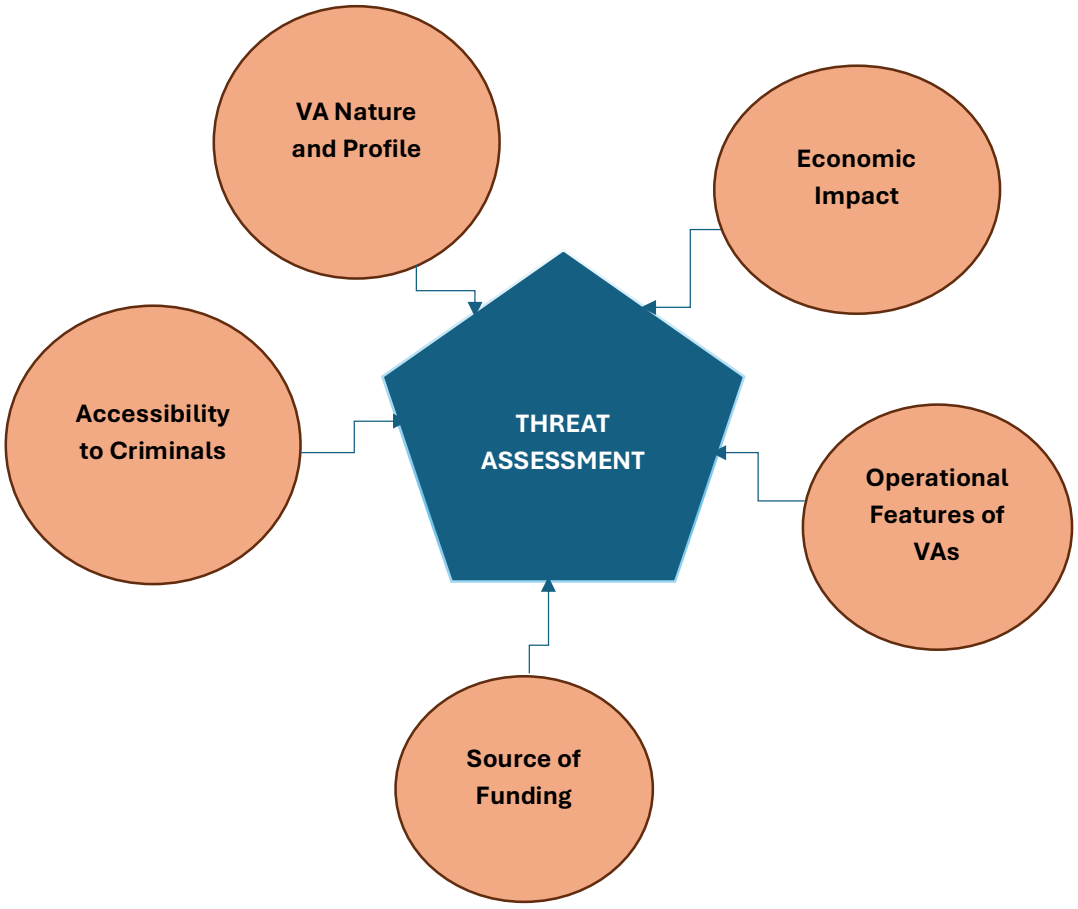
5.2 ML/TF/PF Inherent Threat Assessment from VASP Channels

This section highlights the inherent ML/TF/PF threat assessment of both VAs and VASPs in the Malawian ecosystem. Threat generally refers to a proceed (illicit or licit) generated by a person aimed at exploiting VA activities for ML/TF/PF.

5.2.1 Overall Threat Assessment

The overall inherent ML/TF/PF threat for VAs and VASPs in Malawi was deemed as High. This was attributed to High-risk rating on intermediate variables for VASPs operating in Malawi (Investment Providers, Asset Exchangers and Wallet Providers). The assessment was based on the following five key intermediary variables as depicted in Figure 7 below: -

Figure 7: Intermediary Variables for Inherent Threat Assessments



5.2.2 Investment Providers Threat Assessment

Investment providers are persons that enable investment in or purchases of VAs through a managed investment scheme.

The threat assessment for investment providers in Malawi was rated **high** (67 percent) and only covered platform operators as there was limited data for the other trading platforms and on utilisation of emerging products such as crypto escrow services and crypto custodian services.

The high rating was mainly on account of **very high** ratings on the increased likelihood of *P2P Cross-Border Transfers* for customers or users spread across the globe as well as the absence of face-to-face contact for all VAs provided by the operators. In addition, there was a high likelihood for criminals to integrate dirty money into the VA ecosystem, mainly due to lack of domestic regulation and supervision. The rating was exacerbated by the increased difficulty for LEAs to *trace and seize VAs*, as well as the lack of entry controls for VASPs.

The threat for *TF/PF* was rated as **medium** mainly due to the absence of national standards such as legal framework for VASPs to comply with and government measures to mitigate risks associated with VA activities in Malawi. Similarly, risk ratings for *Collection of Funds*, *Anonymity/Pseudonymity*, and *Speed of Transfer* were rated **high**, mainly due to one Operator offering a decentralised system. Further, the absence of known terrorist individuals, groups or proliferation financers in Malawi at the time of the assessment impacted the likelihood rating for collection of funds. In addition, the lack of relevant data on financial performance of VASPs in Malawi posed a challenge in assessing the extent of the growing sector's impact on monetary policy and associated risks were thus rated **high.** Further, access by criminals to VASP platforms was rated **high** due to high possibility of hacking and weak AML controls by some international VA exchanges facilitating transactions linked to Malawi. Nonetheless, the threat from utilisation of *Centralised System* was rated **very low** as most exchanges in Malawi operate in a centralised environment.

Table 5 below summarises the inherent risk ratings on all the applicable input variables for platform operators: -

Table 5: Inherent Threat Assessment Ratings for Platform Operators

Intermediary variables	Input variables	VIRTUAL ASSET INVESTMENT PROVIDERS
		Trading Platforms
		Platform Operators
VA Nature and Profile	Anonymity/pseudonymity	High Risk
	P2P Cross-Border Transfer and Portability	Very High Risk
	Absence of face-to-face contact	Very High Risk
	Traceability	High Risk
	Speed of Transfer	High Risk
Accessibility to Criminal	Mining by criminal	Low Risk
	Collection of funds	High Risk
	Transfer of funds	Medium Risk
	Dark Web Access	Medium Risk
	Expenditure of funds	Very High Risk
Source of funding VA	Bank or card as source of funding VA	Medium Risk
	Cash transfers, valuable in-kind goods	Not Applicable
	Use of virtual currency	Very High Risk
Operational features of VA	Regulated	Does not exist
	Unregulated	Very High Risk
	Centralised Environment	Very Low Risk
	Decentralised Environments	Does not exist
Ease of criminality	Tax evasion	Very High Risk
	Terrorist/Proliferation financing	Medium Risk
	Disguising criminal proceeds to VA not regulated	Very High Risk
	Trace and Seize Difficulty	Very High Risk
	Circumvent Exchange Control	Very High Risk
Economic Impact	Underground economy – Impact on the country's monetary policy	High Risk
	Allow full integration with the financial services market	High Risk
	Prohibit any interaction between the financial institutions and the VC market	Very High Risk
	High level of the accountability product provider	High Risk

5.2.3 Virtual Asset Exchanges Threat Assessment

VA Exchanges provide a digital online platform facilitating VA transfers and exchange. Exchange may occur between one or more forms of VAs, or between VAs and fiat currency.

The overall threat assessment for VA exchanges was rated high (59 percent) and incorporated both transfer (P2P and P2B) and conversion services (fiat-to-virtual, virtual-to-fiat, and virtual-to-virtual). Transfer services are services that facilitate the movement of VAs from one address or account to another (P2P and P2B[13]). On the other hand, VA conversion services are services that exchange one form of VAs for another or for fiat currency[14]. These services are often offered by VASPs. These transactions involve the transfer of VAs by one user to another (individual or business).

Notably, the *Speed of Transfers* for P2P services was rated **very high** due to the lack of an intermediary and increased utilisation by the general public. The assessment also deemed the possibility of access by criminals to VA mining as **high** due to the lack of entry controls and AML/CFT/CFP measures for VASPs, although one VA exchange collects proof of miners. The individual threat emanating from *Dark Web Access* was rated **high** due to the lack of legislation for market entry and AML/CFT/CFP to prevent VA-enabled cybercrime and ensure compliance by VASPs, although some exchanges subject VA users to sanctions screening utilising various sanctions lists, including United Nations Security Council and Office of Foreign Assets Control to comply with international AML/CFT/CFP Standards.

On the other hand, threats emanating from *Cash Transfers or Valuable in-kind Goods* and anonymous funding for fiat-to-virtual conversion services were respectively deemed **very low** and **low**. This was attributed to the fact that all the fiat deposits to VASPs are processed from regulated entities, through commercial bank accounts or cards and mobile money operator wallets, who are supervised for AML/CFT/CFP compliance. In addition, most VASPs did not have physical offices in Malawi. As such, there was a very low possibility for users to incur courier fees to send valuable in-kind goods for exchange with VAs. Appendix I below indicates the risk rating for all inherent risk input variables for VA exchanges in the county.

5.2.4 Virtual Asset Wallet Provider Threat Assessment

Wallet providers provide custodial (hot wallets) and non-custodial (cold wallets) services for VAs on behalf of clients and facilitate exchanges or transfers between one or more VAs, or between VAs and fiat currencies.

The overall threat assessment for wallet providers was rated high (61 percent). The high rating was mainly on account of very high ratings on the increased likelihood of criminals and terrorists utilising VA wallets for terrorist financing, transfer of funds, collection of funds, expenditure of funds, and illegal dark web access. Similarly, the lack of a legislative framework for VAs and VASPs increased the likelihood for wallet users to circumvent exchange control regulations and disguise criminal proceeds to unregulated VASPs using VAs as kickback payments. However, the assessment established that VASPs in Malawi do not utilise cash payments. To this end, threats from cash transfers by wallet users were rated very low. Table 6 below details risk ratings for each inherent risk input variable for wallet providers in the county: -

[13] Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers

[14] **Ibid**

Table 6: Inherent Threat Assessment Ratings for Wallet Providers

Intermediary variables	Input variables	VIRTUAL ASSET WALLET PROVIDERS
		Custodial Services
		Hot Wallet
VA Nature and Profile	Anonymity/pseudonymity	High Risk
	P2P Cross-Border Transfer and Portability	High Risk
	Absence of face-to-face contact	High Risk
	Traceability	Medium Risk
	Speed of Transfer	Very High Risk
Accessibility to Criminal	Mining by criminal	High Risk
	Collection of funds	Very High Risk
	Transfer of funds	Very High Risk
	Dark Web Access	Very High Risk
	Expenditure of funds	Very High Risk
Source of funding VA	Bank or card as source of funding VA	Medium Risk
	Cash transfers, valuable in-kind goods	Very Low Risk
	Use of virtual currency	High Risk
Operational features of VA	Regulated	Does not exist
	Unregulated	Very High Risk
	Centralised Environment	Very Low Risk
	Decentralised Environments	Does not exist
Ease of criminality	Tax evasion	Very High Risk
	Terrorist/Proliferation financing	Medium Risk
	Disguising criminal proceeds to VA not regulated	Very High Risk
	Trace and Seize Difficulty	Very High Risk
	Circumvent Exchange Control	Very High Risk
Economic Impact	Underground economy – Impact on the country's monetary policy	Medium Risk
	Allow full integration with the financial services market	Very High Risk
	Prohibit any interaction between the financial institutions and the VC market	Very High Risk
	High level of the accountability product provider	High Risk

Across all VASPs channels, Hot Wallets was assessed as the channel posing the highest threat with a rating of **75** percent. This was primarily due to the fact that the transactions are characterised by online access, increased anonymity and ease of cross-border transfers. Table 7 below summarises the threat assessment ratings for all channels: -

Table 7: Inherent Threat Assessment Ratings

VASP	TYPE OF SERVICE	CHANNEL	THREAT RATING
Wallet Providers	Custodial Services	Hot Wallet	High (75%)
Asset Exchanges	Transfer service	P2P	High (71%)
		P2B	High (68%)
	Conversion Services	Fiat to virtual	High (60%)
		Virtual to fiat	High (68%)
		Virtual to Virtual	High (68%)
Investment Providers	Trading Platforms	Platform Operators	High (71%)
Overall, Threat Rating			**High**

6.0 VIRTUAL ASSET INHERENT VULNERABILITY ASSESSMENT

This section highlights the inherent vulnerability assessment of both VAs and VASPs in the Malawian ecosystem with regard to ML/TF/PF. Vulnerabilities refer to weaknesses in the AML/CFT/CFP controls that can be exploited by criminals. The FATF emphasizes the importance of identifying and understanding these vulnerabilities to effectively combat ML/TF/PF.

The assessment evaluated the vulnerability of VA wallet providers, VA exchanges and VA investment providers to ML/TF/PF abuse as these were the only providers applicable in the Malawian context.

6.1 Virtual Asset Wallet Providers

The vulnerability assessment of hot wallets was assessed as **high** (77 percent). The assessment established that hot wallet custodial services permit products such as stablecoins, USDT and BTC to be offered through the online channel. The hot wallets are vulnerable to ML/TF/PF abuse as they can be accessed online, and criminals may use them to store and rapidly transfer illicit proceeds domestically and across the globe. VA hot wallets may facilitate non-face-to-face transactions with potentially high-risk countries. The absence of regulatory oversight of VASPs in Malawi for registration or licencing and sanctioning further heightens the vulnerability of VASPs to ML/TF/PF risk exposure.

Nonetheless, the assessment established that the possibility of anonymity of transactions is low as the VASPs do not have Anonymity Enhanced Cryptocurrency (AEC) products, conduct KYC/Enhanced Due Diligence (EDD) processes and are not exposed to Internet Protocol (IP) anonymizers. Further, the VASPs have risk mitigating measures, including adherence to travel rule requirements, conducting risk assessments, sanctions screening, use of centralised platforms and closed loop operating models. The mitigating measures as implemented by the VASPs are however yet to be tested by regulatory and supervisory authorities due to the absence of regulatory and supervisory frameworks. Specific details on ratings for all applicable input variables are indicated in Table 8 below: -

Table 8: VA Wallet Providers Vulnerability Assessment

Vulnerability Input Variable	Hot Wallet
Licensed in the country or abroad	Does not exist
Nature, size and complexity of business	High Risk
Products/services	High Risk
Methods of delivery of products/services	High Risk
Customer types	High Risk
Country risk	High Risk
Institutions dealing with VASP	High Risk
VA (Anonymity/pseudonymity)	High Risk
Rapid transaction settlement	Very High Risk
Dealing with unregistered VASP from overseas	Very High Risk

6.2 Virtual Asset Exchanges

The analysis of the VA exchanges considered transfer and conversion services. Transfer services included P2P and P2B channels, whereas, conversion services included fiat-to-virtual, virtual-to-fiat and virtual-to-virtual channels. The overall vulnerability assessment of VA exchanges was rated **high**.

The assessment noted that VA exchanges accessed by Malawians included both local and global platforms and operated without licencing, registration, or AML/CFT/CFP oversight. The lack of licencing hinders information exchange, monitoring, and accountability. An example of some of the identified VAs offered by the VA exchanges in Malawi include Bitcoin, USDT (Stablecoin), and other cryptocurrencies which support instant global transfers and low fees, amongst other factors. It was noted that it is possible for such high-speed transfers to also hinder intervention or tracing given that they are not subjected to AML/CFT/CFP requirements. At the moment there is no monitoring infrastructure which exists locally to detect any kind of red flags in real time.

VA exchanges also enable cross-border transactions as per the nature of their products. For example, P2P and P2B transactions can be completed between two accounts or individuals in two different jurisdictions almost immediately. Further, the VA exchanges engage with VASPs in foreign jurisdictions that may not have relevant legal frameworks. This poses a **high** vulnerability of untraceable activities, including transfer and conversion of illicit proceeds. However, the assessment noted that some of the exchanges implemented risk-based controls such as conducting risk assessments and KYC. The extent of the risk-based controls and measures were not assessed due to the absence of a regulatory and supervisory framework.

The *Products and Services* being offered were assessed to be inherently posing **high** vulnerability as they involve non-face-to-face domestic and cross-border transactions through

online platforms. The services are unregulated and offer anonymity features. Services offered by VA exchanges in Malawi are delivered through remote digital channels, such as mobile applications and social media-based trading, including WhatsApp, Facebook and Telegram. Although the VA exchanges have internal controls such as sanction screening, travel rule and EDD, it is possible that they also operate in TF/PF high-risk countries. Nonetheless, the assessment established that the possibility of anonymity of transactions is low as the VA exchanges implement KYC processes, do not have AEC products and are not exposed to IP anonymizers. Further the VA exchanges do not collaborate with unlicensed or unregistered merchant platforms. Table 9 below details vulnerability ratings for all applicable input variables: -

Table 9:VA Exchanges Vulnerability Assessment

Vulnerability Input Variable	**Transfer Services**		**Conversion Services**		
	P2P	**P2B**	**Fiat-to-Virtual**	**Virtual-to-Fiat**	**Virtual-to-Virtual**
Licensed in the country or abroad	Does not exist	Does not exist	Does not exist	Does not exist	Does not exist
Nature, size and complexity of business	High Risk	High Risk	High Risk	High Risk	High Risk
Products/services	High Risk	High Risk	High Risk	High Risk	High Risk
Methods of delivery of products/services	High Risk	High Risk	Medium Risk	High Risk	High Risk
Customer types	High Risk	High Risk	Medium Risk	High Risk	High Risk
Country risk	High Risk	High Risk	High Risk	High Risk	High Risk
Institutions dealing with VASP	High Risk	Low Risk	Low Risk	Low Risk	Low Risk
VA (Anonymity/pseudonymity)	High Risk	Low Risk	Low Risk	Low Risk	Low Risk
Rapid transaction settlement	Very High Risk	High Risk	High Risk	High Risk	High Risk
Dealing with unregistered VASP from overseas	Very High Risk	Very High Risk	Very High Risk	Very High Risk	Very High Risk

6.3 Investment Providers

The assessment established that the available unlicensed/unregistered VASPs present in Malawi do not offer investment services. However, VA users in Malawi access investment services from international VASPs using online channels.

The vulnerability to ML/TF/PF risk for investment providers' trading platforms was rated **high** due to their *nature, size and business complexity* as they are globally accessible to users online, such that criminals may use them to invest and rapidly settle illicit proceeds. Additionally, VA investment platforms facilitate non-face-to-face investment transactions with potentially high-risk customers and countries linked with TF/PF, child trafficking and smuggling activities. The absence of entry controls, regulatory oversight for VASPs and sanctioning of unlicenced/unregistered VASPS in Malawi further increases the vulnerability of platform operators to ML/TF/PF risk exposure. In addition, the assessment noted a case of AML/CFT/CFP breaches by one of the investment providers as detailed below: -

Case 4: Binance AML/CFT/CFP Breaches in USA[15]

In November 2023, Binance Holdings Limited and its affiliates, which operate the world's largest VASP, Binance.com, entered into the largest resolutions in the US Treasury's history with FinCEN (including a penalty of $3.4 billion) and OFAC (including a penalty of nearly $1 billion), as well as resolutions of parallel investigations by the US Department of Justice and the Commodity Futures Trading Commission. As part of these resolutions, Binance pleaded guilty and paid penalties totalling over $4.3 billion, to resolve violations under the Bank Secrecy Act (BSA).

This case focused on some key allegations and violations such as AML failures whereby Binance was accused of willfully failing to implement an effective AML program, violating the BSA. This lapse allowed illicit actors, including terrorist organizations like Hamas, Al Qaeda, and ISIS, to transact on the platform. Further, the VA exchange facilitated transactions with users in sanctioned jurisdictions such as Iran, North Korea, Syria, and the Crimea region of Ukraine, contravening the International Emergency Economic Powers Act (IEEPA). They also operated as an unregistered money transmitting business and illegally offered digital asset derivatives to U.S. customers without proper registration.

Details of all applicable input variable for vulnerability ratings are indicated in Table 10 below: -

[15] USA NRA Report - https://www. justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution

Table 10: VA Investment Providers Assessment

Vulnerability Input Variable	Platform Operators Risk Rating
Licensed in the country or abroad	Does not exist
Nature, size and complexity of business	Very High Risk
Products/services	High Risk
Methods of delivery of products/services	High Risk
Customer types	Very High Risk
Country risk	Very High Risk
Institutions dealing with VASP	High Risk
VA (Anonymity/pseudonymity)	High Risk
Rapid transaction settlement	Very High Risk
Dealing with unregistered VASP from overseas	Very High Risk

Across all VASPs channels, Platform Operators were assessed as the most vulnerable channels with respective ratings of **83** percent. This was primarily due to associated increased anonymity, lack of regulation and ease of cross-border transfers. Table 11 below summarises ratings for the applicable VA channels' vulnerability: -

Table 11: Inherent Vulnerability Assessment Ratings

VASP	TYPE OF SERVICE	CHANNEL	VULNERABILITY RATING
Wallet Providers	Custodial Services	Hot Wallet	High (77%)
Asset Exchanges	Transfer service	P2P	High (77%)
		P2B	High (67%)
	Conversion Services	Fiat to virtual	High (63%)
		Virtual to fiat	High (67%)
		Virtual to Virtual	High (67%)
Investment Providers	Trading Platforms	Platform Operators	High (83%)
Overall Vulnerability Rating			**High**

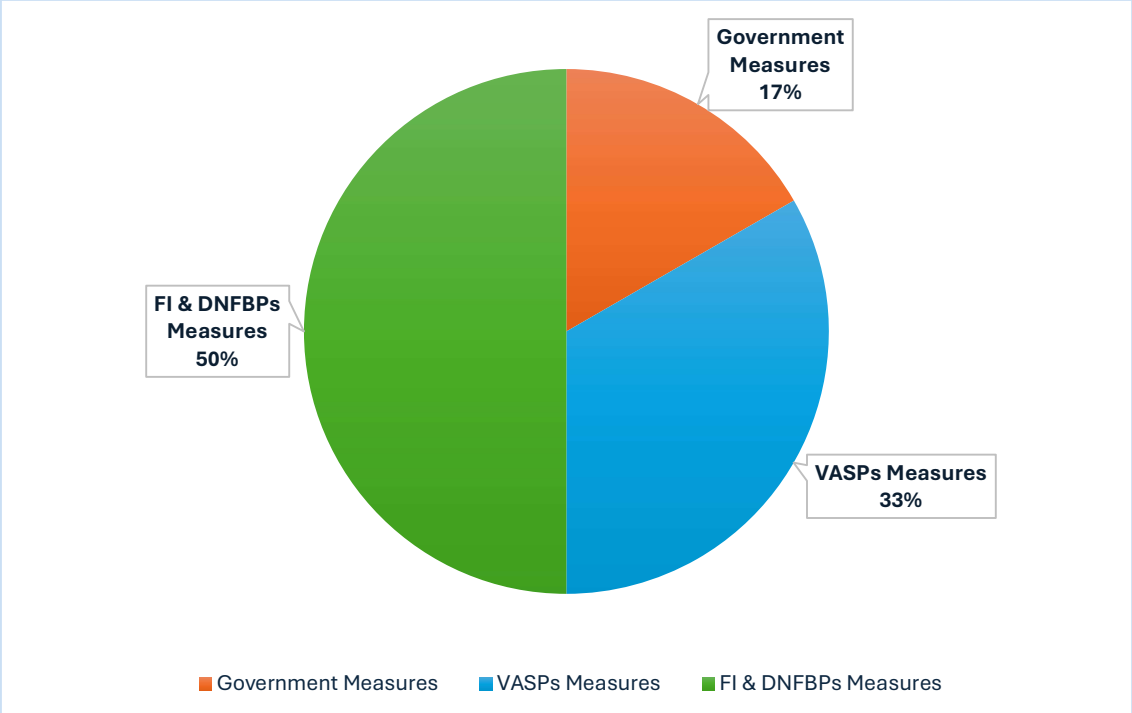
7.0 MITIGATION MEASURES FOR VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

This section evaluates the adequacy and effectiveness of the existing AML/CFT/CFP frameworks implemented by the government bodies, including LEAs and Supervisory authorities, TOEs, and VASPs in addressing the threats and vulnerabilities identified above. Overall, the mitigating measures were assessed as very low.

7.1 Overview

The analysis evaluated the adequacy and effectiveness of existing AML/CFT/CFP mitigation measures across various sectors, including government bodies, VASPs, and traditional obliged entities such as FIs and DNFBPs. Each sector was assessed individually to determine its level of compliance before assigning an overall mitigation rating. Figure 8 below presents a visual representation of the assessment of the mitigation measures implemented by each sector in Malawi: -

Figure 8: Mitigation Measures Assessment by Sector[16]



The overall mitigation measures across all assessed sectors was rated as **very low**. Government bodies exhibited critically inadequate measures, lacking the fundamental legal, regulatory, and institutional frameworks necessary for effective AML/CFT/CFP efforts. VASPs displayed significant deficiencies, particularly in governance and transparency, with minimal oversight

[16] Low scores indicate weaker measures

and limited compliance initiatives. While FIs and DNFBPs perform slightly better, their risk mitigation practices remain inadequate and are inconsistently implemented, offering only marginal protection against financial crime in general, and VA activities in particular. Collectively, these findings highlight a systemic deficiency in the country's AML/CFT/CFP preparedness, as all sectors demonstrate inadequate capacity to effectively manage and mitigate existing risks.

7.2 Government Mitigation Measures

The government's overall mitigation response was rated as **very low** and measures put in place were identified as the weakest among the sectors assessed. In Malawi, key fundamental elements, including the legal, regulatory, and institutional frameworks, are non-existent. The sole mitigating measure in place is the capacity of law enforcement agencies to address virtual asset-related issues; however, the capacity is limited and has therefore been assessed as providing only a **low** level of mitigation. This challenge is further compounded by the absence of international cooperation mechanisms and the lack of tailored AML/CFT/CFP national and regulatory guidance for VAs and VASPs.

7.3 VASPs Mitigation Measures

Mitigation measures within the VASP sector exhibited consistent weaknesses, particularly in the areas of transparency and governance, both of which have been assessed as **very low**. Although there are emerging efforts aimed at improving compliance, including limited training initiatives and preliminary attempts to align with international standards, these measures remain fragmented and insufficient to meaningfully address the substantial governance and transparency-related risks. While VASPs demonstrated marginally stronger mitigation efforts compared to government institutions, these remain inadequate and have not been comprehensively tested by competent supervisory authorities.

7.4 FIs and DNFBPs

The overall level for mitigation for FIs and DNFBPs was rated **medium** as TOEs had put in place relatively adequate measures as compared to government bodies and VASPs. These entities have established some foundational risk management and compliance mechanisms, such as KYC/CDD procedures, compliance functions and internal reporting systems. The level of mitigation measures established by FIs was rated **high.** On the other hand, the level for measures under DNFBPs was rated **low**; mainly due to notable deficiencies in both implementation and operational effectiveness.

Key challenges included inconsistent application of AML/CFT/CFP controls, limited staff training, and inadequate monitoring and enforcement by supervisory authorities. Furthermore, the absence of sector-specific guidance and limited technological integration hinders the entities' ability to detect and respond to VA emerging risks effectively. While the existence of basic frameworks is a positive development, the medium rating highlights the need for enhanced regulatory oversight, improved institutional capacity, and stronger compliance cultures to align with international AML/CFT/CFP standards.

8.0 OVERALL COUNTRY RISK

Given the preceding assessment of high overall threat exposure, high overall vulnerability exposure, and low overall effectiveness rating of national mitigating measures by Government, VASPs and TOEs, the overall exposure of Malawi to ML/TF/PF risks arising from VAs and VASPs was rated **high**.

The threat factors range from the nature and profile of VAs, accessibility to criminals, operational features of VA and economic impact. The vulnerability factors were with respect to the type of VA and their products and services. Specifically, key considerations included:

i. The underlying technology of VA and its features which may increase pseudonymity and anonymity, thereby complicating the detection of criminal activity;
ii. Cross-border transfer and portability of VA which may make it attractive to criminals who can receive and make payments from anywhere in the world without having to pass through regulated institutions;
iii. VAs are largely traded online characterized by non-face-to-face customer relationships which may permit anonymity;
iv. VAs anonymity that may make traceability a challenge;
v. Absence of VA and VASPs regulation and supervision; and
vi. Speed of funds transfer which may increase TF/PF risks on account that the funds may be transferred to or from high-risk jurisdictions and unregulated VASPs.

Despite mitigating measures by Government, VASPs and TOEs, including KYC/CDD; utilisation of centralized systems; and capacity building efforts for LEAs and other competent authorities to investigate, trace and seize VAs, these measures are not adequate to mitigate the ML/TF/PF risks associated with VAs. Generally:

i. No adequate supervision and monitoring mechanism of VASPs because of absence of relevant legal and regulatory framework;
ii. No international cooperation between Malawi and other countries on VAs; and
iii. Regulated financial institutions may offer higher mitigation measures, DNFBPs measures are inadequate.

Table 12 below summarises the overall VA and VASP ML/TF/PF risk rating for Malawi: -

Table 12: Overall VAs and VASPs ML/TF/PF Risk Rating for Malawi

VASP, SERVICE, CHANNEL			OVERALL VA/VASP RISK ML/TF/PF RATING				
VASP	**Type of Service**	**Channel**	**Inherent Threat**	**Inherent Vulnerability**	**Total Risk**	**Mitigating Measures (Level)**	**Residual Risk**
Virtual Asset Wallet Providers	Custodial Services	Hot Wallet	High	High	High	Low	High
Virtual Asset Exchanges	Transfer Services	P2P	High	High	High	Low	High
		P2B	High	High	High	Low	High
	Conversion Services	Fiat-to-Virtual	High	High	High	Low	High
		Virtual-to-Fiat	High	High	High	Low	High
		Virtual-to-Virtual	High	High	High	Low	High
Virtual Asset Investment Providers	Trading Platforms	Platform Operators	High	High	High	Low	High

Specific details on inherent threat and vulnerability ratings for all the assessed VA channels are indicated in appendices II to VIII.

9.0 CONCLUSION AND RECOMMENDATIONS

The risk assessment has established that Malawi faces a **high** overall risk of ML/TF/PF stemming from the growing use of VAs and VASPs. The increased exposure was largely attributed to the absence of entry controls, regulatory and supervisory frameworks, inadequate institutional capacity, and the increasing accessibility and adoption of virtual asset platforms—many of which operated outside the purview of domestic oversight. The inherent features of VAs, such as anonymity, speed, and cross-border functionality, significantly heighten the risk of abuse by criminals and other illicit players. Mitigation measures adopted by some TOEs and VASPs were very limited, in the absence of a robust legislation, their efforts were uncoordinated and insufficient to address the scale and complexity of the associated risks.

Considering the evolving technologies and increasing innovations in the global financial sector landscape, it is apparent that the utilisation of VAs in Malawi and the persuasion to tap into the highly latent market niche shall continue to grow. To this end, and based on the findings of the assessment, it is recommended that Malawi:

i. Urgently defines a clear policy stance to allow VAs and VASPs and provide the necessary legislative environment for this, in accordance with international standards and practices;

ii. Implements training and awareness programs among law enforcement agencies, regulatory and supervisory authorities, the private sector and the general public on risks associated with VAs and VASPs to enable them carry out their AML/CFT/CFP obligations effectively;

iii. Enhances cooperation and information sharing with domestic and international agencies and organizations to benefit from the latest developments related to dealings with VAs and VASPs; and

iv. Develops the necessary procedures for investigating, prosecuting, seizing, confiscating, and managing VAs associated with illicit activities.

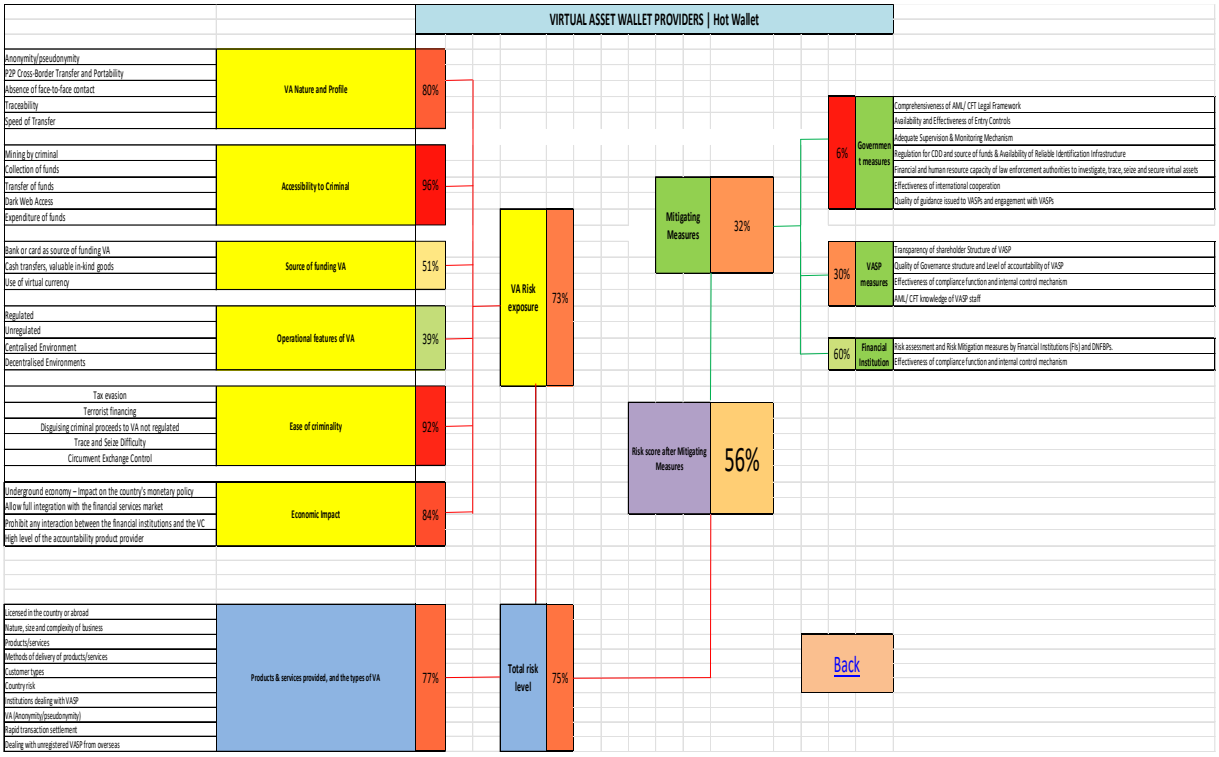
10.0 APPENDICES

Appendix I: Inherent Threat Assessment Ratings for Platform Operators

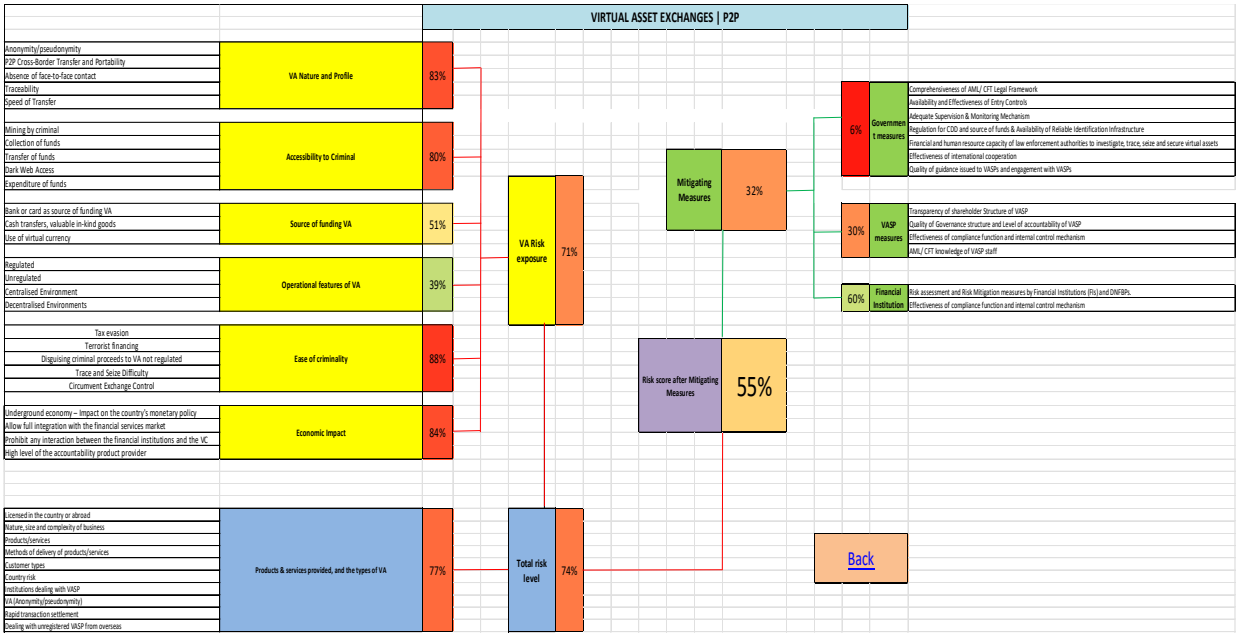
Intermediary variables	Input variables	VIRTUAL ASSET EXCHANGES				
		Transfer Services		Conversion Services		
		P2P	P2B	Fiat-to-Virtual	Virtual-to-Fiat	Virtual-to-Virtual
VA Nature and Profile	Anonymity/pseudonymity	High Risk	Medium Risk	Low Risk	Medium Risk	Medium Risk
	P2P Cross-Border Transfer and Portability	High Risk	High Risk	Medium Risk	High Risk	High Risk
	Absence of face-to-face contact	High Risk	High Risk	Medium Risk	High Risk	High Risk
	Traceability	High Risk	High Risk	Medium Risk	High Risk	High Risk
	Speed of Transfer	Very High Risk	High Risk	Medium Risk	High Risk	High Risk
Accessibility to Criminal	Mining by criminal	High Risk	High Risk	Medium Risk	High Risk	High Risk
	Collection of funds	High Risk	High Risk	Medium Risk	High Risk	High Risk
	Transfer of funds	High Risk	High Risk	Medium Risk	High Risk	High Risk
	Dark Web Access	High Risk	High Risk	Medium Risk	High Risk	High Risk
	Expenditure of funds	High Risk	High Risk	Medium Risk	High Risk	High Risk
Source of funding VA	Bank or card as source of funding VA	Medium Risk	Low Risk	Low Risk	Low Risk	Low Risk
	Cash transfers, valuable in-kind goods	Very Low Risk	Very Low Risk	Very Low Risk	Very Low Risk	Very Low Risk
	Use of virtual currency	High Risk	High Risk	Medium Risk	High Risk	High Risk
Operational features of VA	Regulated	Does not exist	Does not exist	Does not exist	Does not exist	Does not exist
	Unregulated	Very High Risk	Very High Risk	Very High Risk	Very High Risk	Very High Risk

	Centralised Environment	Very Low Risk	Very Low Risk	Very Low Risk	Very Low Risk	Very Low Risk
	Decentralised Environments	Does not exist	Does not exist	Does not exist	Does not exist	Does not exist
Ease of criminality	Tax evasion	Very High Risk	Very High Risk	Very High Risk	Very High Risk	Very High Risk
	Terrorist/proliferation financing	Medium Risk	Medium Risk	Medium Risk	Medium Risk	Medium Risk
	Disguising criminal proceeds to VA not regulated	High Risk	High Risk	High Risk	High Risk	High Risk
	Trace and Seize Difficulty	Very High Risk	Very High Risk	Very High Risk	Very High Risk	Very High Risk
	Circumvent Exchange Control	Very High Risk	Very High Risk	Very High Risk	Very High Risk	Very High Risk
Economic Impact	Underground economy – Impact on the country's monetary policy	Medium Risk	Low Risk	Low Risk	Low Risk	Low Risk
	Allow full integration with the financial services market	Very High Risk	Very High Risk	Very High Risk	Very High Risk	Very High Risk
	Prohibit any interaction between the financial institutions and the VC market	Very High Risk	Very High Risk	Very High Risk	Very High Risk	Very High Risk
	High level of the accountability product provider	High Risk	High Risk	High Risk	High Risk	High Risk

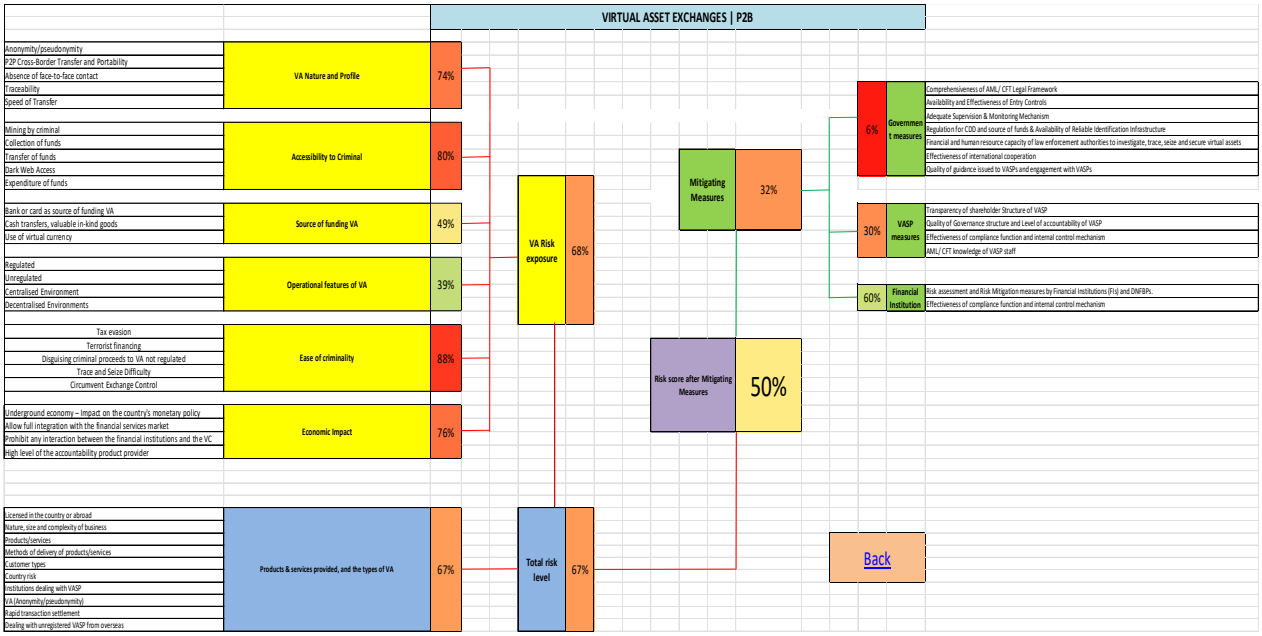
Appendix II: Risk Assessment Ratings for Hot Wallet Providers



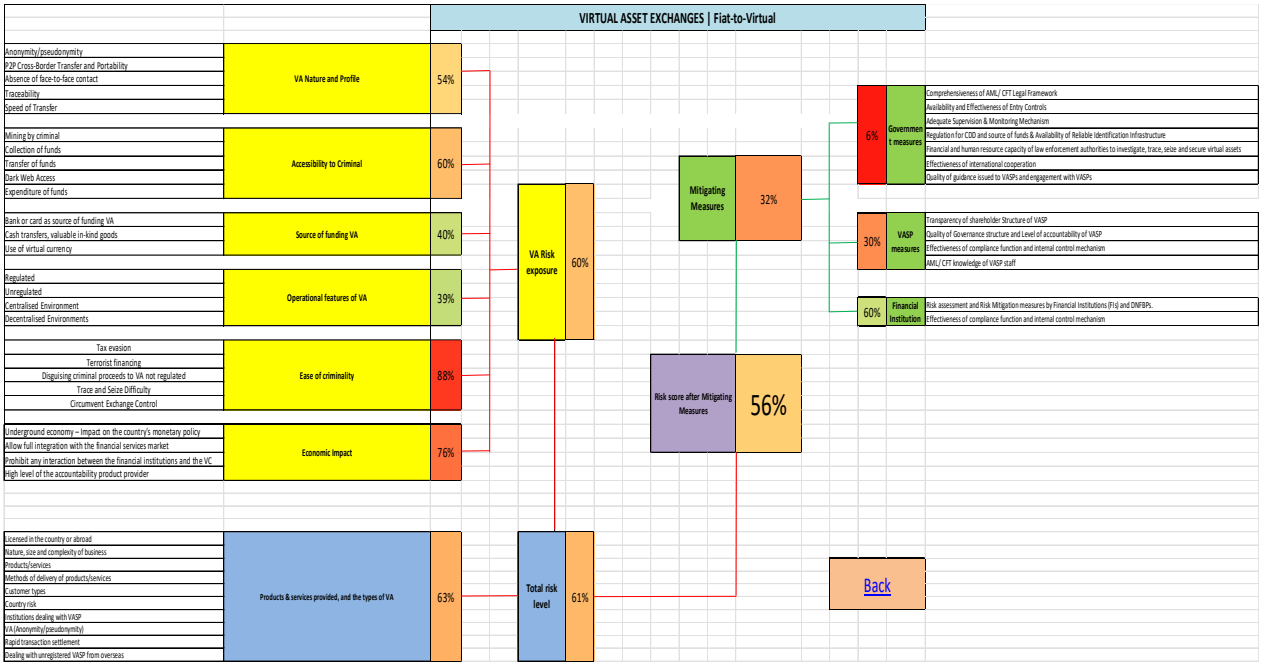
Appendix III: Risk Assessment Ratings for P2P Virtual Asset Exchanges



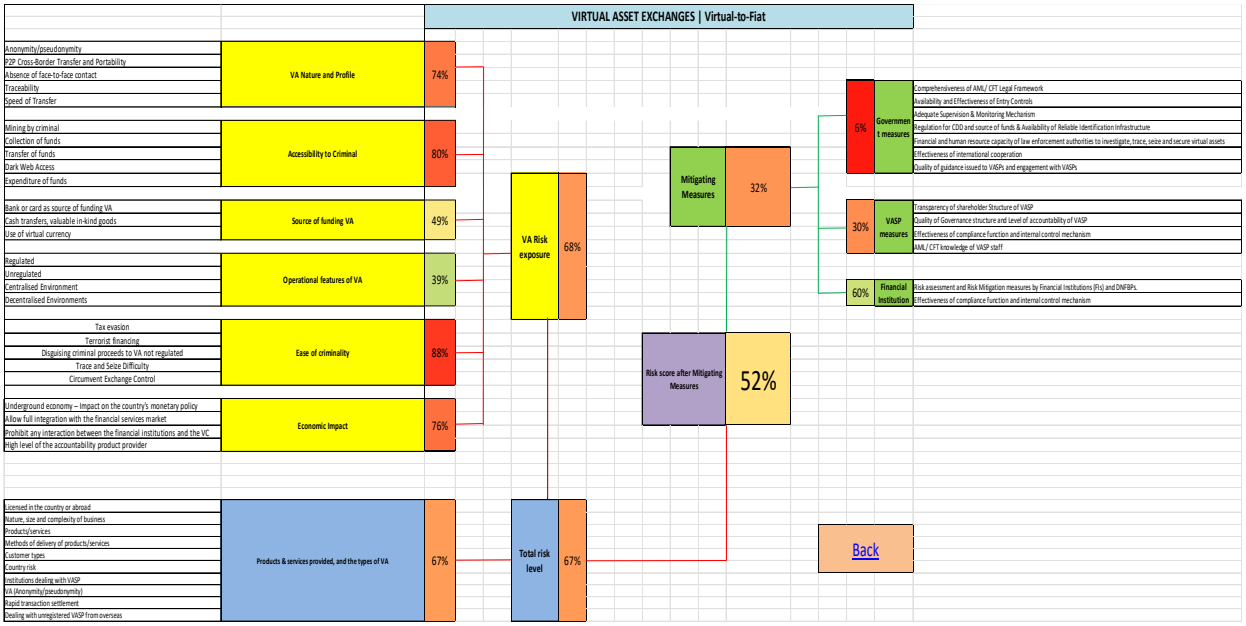
Appendix IV: Risk Assessment Ratings for P2B Virtual Asset Exchanges



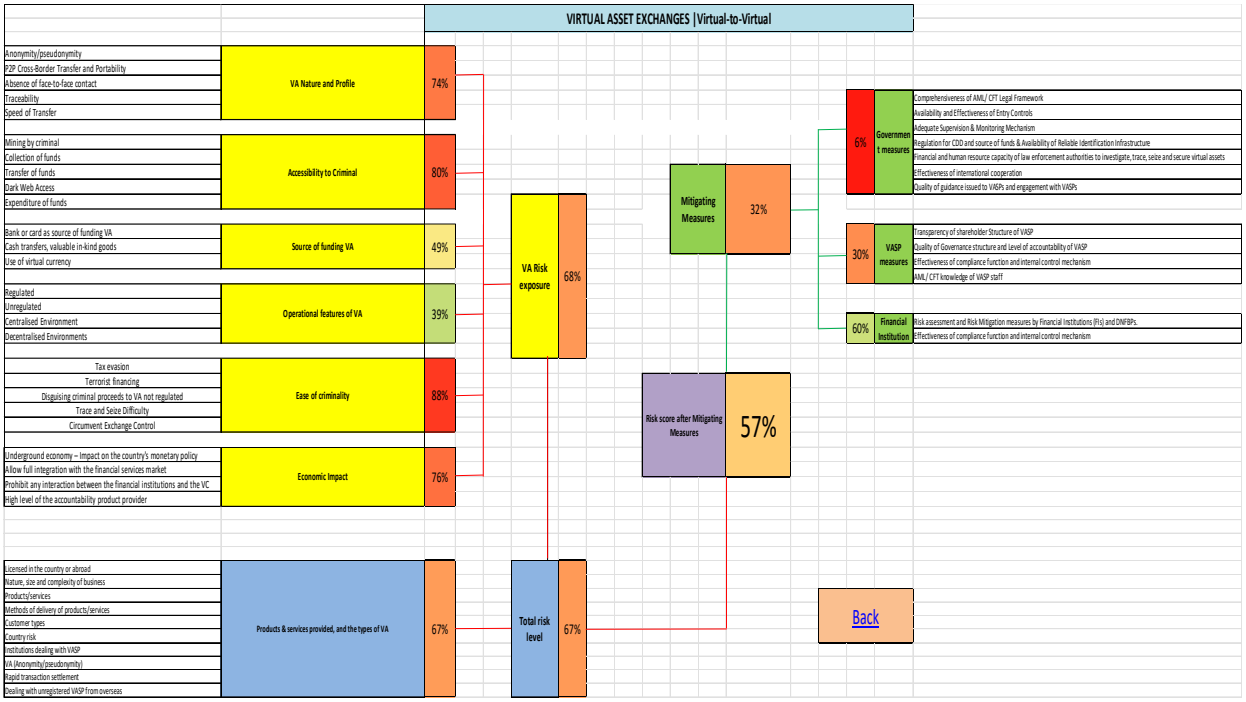
Appendix V: Risk Assessment Ratings for Fiat-to-Virtual, Virtual Asset Exchanges



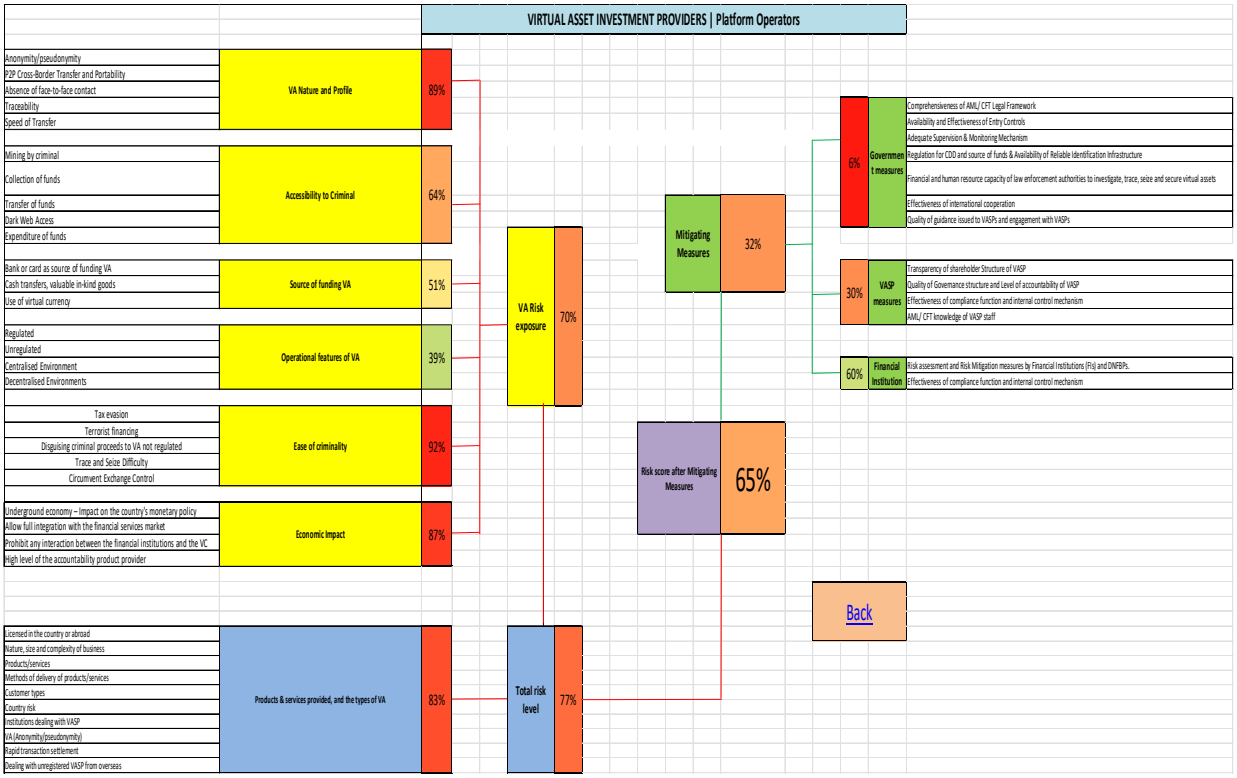
Appendix VI: Risk Assessment Ratings for Virtual-to -Fiat, Virtual Asset Exchanges



Appendix VII: Risk Assessment Ratings for Virtual-to -Virtual, Virtual Asset Exchanges



Appendix VIII: Risk Assessment Ratings for Virtual Asset Investment Providers, Platform Operators,



11.0 REFERENCES

1. Chainalysis - The 2024 Geography of Crypto Report

2. Crypto-Assets Activity around the World Evolution and Macro-Financial Drivers; Policy Research Working Paper 2022- World Bank Document

3. Crypto Market Sizing Report 2024

4. Cryptocurrency Ownership Data 2024 - https://www.triple-a.io/cryptocurrency-ownership-data

5. DOJ, "Binance and CEO Plead Guilty to Federal Charges in $4B Resolution," (November 21, 2023), https://www.justice.gov/usao-wdwa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution

6. FATF Glossary: https://www.fatf-gafi.org/en/pages/fatf-glossary.html#accordion-a13085a728-item-dd6de709ef

7. FATF Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity – https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/VACG-Table-Jurisdictions-2024.pdf.coredownload.pdf

8. FATF 2021 Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers

9. FATF 2024 Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs

10. MBC Digital - https://www.facebook.com/mbctv.malawi/posts/fiscal-and-fraud-section-of-the-malawi-police-service-informs-the-general-public/1752886008147183/

11. Malawi Mutual Evaluation Report 2019 - https://www.esaamlg.org/index.php/Mutual_Evaluations/readmore_me/427

12. IMF 2024 - ASAP: A Conceptual Model for Digital Asset Platforms

13. Survey Report on The Opportunities and Challenges Posed by Virtual Assets and Virtual Assets Service Providers in the Eastern and Southern Africa Anti-Money Laundering (ESAAMLG) Region – June 2024

14. The Registrar of Financial Institution Annual Report 2023.

15. Targeted Update on Implementation of The FATF Standards on Virtual Assets And Virtual Asset Service Providers - https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf
16. VASP Registrations Hit Record Highs Coin-cub Unveils the VASP Report 2024 - https://coincub.com/vasp-registration-report-2024-coincub/

17. WikiCypto News - Legal Perspectives on Fraudulent Bitcoin Activities in Malawi